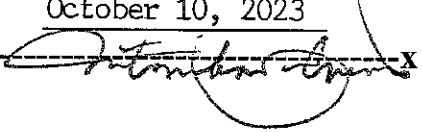


EN BANC

A.M. No. RTJ-20-2579 [Formerly A.M. No. 20-06-75-RTC] — OFFICE OF THE COURT ADMINISTRATOR, Petitioner, v. JUDGE EDRALIN C. REYES, PRESIDING JUDGE, BRANCH 43, REGIONAL TRIAL COURT, ROXAS CITY, ORIENTAL MINDORO, Respondent.

Promulgated:

October 10, 2023

X-----X

SEPARATE CONCURRING OPINION

LEONEN, J.:

I concur. Judge Edralin C. Reyes should be dismissed from service for soliciting bribes from lawyers, litigants, and government officials¹—acts tantamount to gross misconduct—and be liable for simple misconduct by failing to keep a proper record- and evidence-keeping system in his courts.²

To weaken the charge of gross misconduct against him, Judge Reyes raises the alleged violation of his constitutional right to privacy when his personal communications were retrieved from a laptop assigned to him by this Court and used in evidence against him.³

Undoubtably, the right to privacy is a basic human right, enshrined in no less than the Constitution and international human rights instruments, and reinforced in our jurisprudence:

The right to privacy is part and parcel of basic human rights as seen in both the United Nations Declaration of Human Rights and International Covenant on Civil and Political Rights, which protect against the “arbitrary interference with . . . privacy.” In particular, the United Nations Declaration of Human Rights provides:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

¹ *Ponencia*, p. 34.

² *Id.* at pp. 36–37.

³ *Id.* at 21.



In *Morfe v. Mutuc*, this Court recognized the fundamental right to privacy, or the “right to be let alone,” to be independent from the right to liberty and, “in itself, ...is fully deserving of constitutional protection”:

There is much to be said for this view of Justice Douglas: “Liberty in the constitutional sense must mean more than freedom from unlawful governmental restraint; it must include privacy as well, if it is to be a repository of freedom. The right to be let alone is indeed the beginning of all freedom.” As a matter of fact, this right to be let alone is, to quote from Mr. Justice Brandeis “the most comprehensive of rights and the right most valued by civilized [individuals].”

The right to privacy and its other facets are also expressly protected in various provisions of the Bill of Rights:

Section 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.

Section 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

Section 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

....

Section 6. The liberty of abode and of changing the same within the limits prescribed by law shall not be impaired except upon lawful order of the court. Neither shall the right to travel be impaired except in the interest of national security, public safety, or public health, as may be provided by law.

....

Section 8. The right of the people, including those employed in the public and private sectors, to form unions, associations, or societies for purposes not contrary to law shall not be abridged.

....

Section 17. No person shall be compelled to be a witness against himself.

As the right to privacy is a fundamental right guaranteed by the Constitution, the State has the burden of proving that its intrusion into the zones of privacy is “justified by some compelling state interest and that it is narrowly drawn.”

The relevance of the zones of privacy to the right of privacy was discussed in *In re Sabio*:

Zones of privacy are recognized and protected in our laws. Within these zones, any form of intrusion is impermissible unless excused by law and in accordance with customary legal process. The meticulous regard we accord to these zones arises not only from our conviction that the right to privacy is a “constitutional right” and “the right most valued by civilized [individuals],” but also from our adherence to the Universal Declaration of Human Rights which mandates that, “no one shall be subjected to arbitrary interference with his privacy” and “everyone has the right to the protection of the law against such interference or attacks.”

Our Bill of Rights, enshrined in Article III of the Constitution, provides at least two guarantees that explicitly create zones of privacy. It highlights a person's “right to be let alone” or the “right to determine what, how much, to whom and when information about [themselves] shall be disclosed.” Section 2 guarantees “the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures of whatever nature and for any purpose.” Section 3 renders inviolable the “privacy of communication and correspondence” and further cautions that “any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.”⁴ (Citations omitted)

Nonetheless, the right to privacy is not absolute. A person's privacy may be lawfully transgressed upon a finding that there was no reasonable expectation of privacy in the person's act or conduct:

The reasonableness of a person's expectation of privacy depends on a two-part test: (1) whether by his conduct, the individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable. The factual circumstances of the case determines the reasonableness of the expectation. However, other factors, such as customs, physical surroundings and practices of a particular activity, may serve to create or diminish this expectation.⁵

In this day and age, mobile phones are no longer merely devices with which to make and answer calls, and send and receive SMS or MMS. Technological developments coupled with social, cultural, and economic

⁴ J. Leonen, Separate Concurring Opinion in *Philippine Stock Exchange Inc. et al. v. Secretary of Finance et al.*, G.R. No. 213860, July 5, 2022 [Per J. Hernando, *En Banc*].

⁵ *Ople v. Torres*, 354 Phil. 948, 980-981 (1998) [Per J. Puno, *En Banc*].

changes have made it so that mobile phones now act as gateways to accessing the internet for information and social interaction; repositories of memories immortalized in photos and videos; portals for banking and financial transactions; and even portable workstations with computing power equivalent or better than much larger laptops and desktop computers.

Mobile phones now contain so much data that they are vectors of financial fraud, identity theft, and other misuses of personal information, including sensitive personal information. In consideration of the ever-evolving risks associated with retaining these data in a single device, mobile phone manufacturers and application developers have incorporated many technological measures into mobile phones for the purpose of keeping mobile phone data safe from the reach of unwanted and unscrupulous third parties. The use of measures such as data encryption, passwords, and other unique identity tokens, and multifactor authentication including biometrics and facial recognition, can be seen as mobile phone owners exhibiting that they do have an expectation of privacy in their mobile phones and their data.

Further, our laws have recognized that the expectation of privacy in mobile phones is a reasonable one.

Republic Act No. 8792, the Electronic Commerce Act of 2000, states that access to electronic files must be authorized:


SECTION 31. Lawful Access. — Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key[.]

Hacking or cracking computer⁶ systems is punishable under the Electronic Commerce Act:

SECTION 33. Penalties. — The following Acts shall be penalized by fine and/or imprisonment, as follows:

⁶ Republic Act No. 8792 defines a “computer” in section 5(5)(b) as:
SECTION 5(b). Definition of Terms. — For the purposes of this Act, the following terms are defined, as follows:

....
(b) “Computer” refers to any device or apparatus singly or interconnected which, by electronic, electro-mechanical, optical and/or magnetic impulse, or other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.



(a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communication system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents shall be punished by a minimum fine of One hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years[.]

Republic Act No. 10175, the Cybercrime Prevention Act, includes mobile phones and smart phones within its definition of a “computer” for the law’s purposes.⁷ As such, illegal access of mobile phones,⁸ and data interference with computer data stored in mobile phones⁹ are criminal offenses.

Moreover, this Court has also issued the A.M. No. 17-11-03-SC, the Rule on Cybercrime Warrants, which includes provisions on the issuance and implementation of warrants on search, seizure, and examination of computer data, including data in mobile phones:

Section 6.1. Warrant to Search, Seize and Examine Computer Data (WSSECD). — A Warrant to Search, Seize and Examine Computer Data (WSSECD) is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to search the particular place for items to be seized and/or examined.

⁷ Republic Act No. 10175, sec. 3(d), which states:
SEC. 3. Definition of Terms. — For purposes of this Act, the following terms are hereby defined as follows:

....

(d) Computer refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks and other devices connected to the internet.

⁸ Republic Act No. 10175, sec. 4(a)(1), which states:
SEC. 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

....

(1) Illegal Access. — The access to the whole or any part of a computer system without right. ...

⁹ Republic Act No. 10175, sec. 4(a)(3), which states:
SEC. 4. Cybercrime Offenses. — The following acts constitute the offense of cybercrime punishable under this Act:

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

....

(3) Data Interference. — The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

Section 6.2. Contents of Application for a WSSECD. — The verified application for a WSSECD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the computer data sought to be searched, seized, and examined, and all other items related thereto. In addition, the application shall contain an explanation of the search and seizure strategy to be implemented, including a projection of whether or not an off-site or on-site search will be conducted, taking into account the nature of the computer data involved, the computer or computer system's security features, and/or other relevant circumstances, if such information is available.

....

Section 6.5. Allowable Activities During the Implementation of the WSSECD. — Pursuant to Section 15, Chapter IV of RA 10175, the interception of communications and computer data may be conducted during the implementation of the WSSECD: Provided, that the interception activities shall only be limited to communications and computer data that are reasonably related to the subject matter of the WSSECD; and that the said activities are fully disclosed, and the foregoing relation duly explained in the initial return.

Likewise, law enforcement authorities may order any person, who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the search, seizure and examination.

Here, however, Judge Reyes' own acts negated both his individual expectation of privacy, as well as the Court's duty to respect that expectation.

As stated in the *ponencia*, the discovery of Judge Reyes' misconduct started with an iPhone backup stored in a laptop assigned to him, later re-assigned to another judge, who turned it over to this Court's Management Information Systems Office (MISO) for repair or replacement:

On 8 August 2018, the Supreme Court assigned a laptop, HP 240 G6 with serial number 5CD7525ZNo (subject laptop) to respondent Judge Edralin Reyes (respondent Judge), then Acting Presiding Judge of Branch 39, RTC, Roxas City, Oriental Mindoro. The subject laptop was transferred to Judge Josephine Carranzo (Judge Carranzo) upon her appointment to Branch 39. On 27 December 2019, Judge Carranzo returned the subject laptop to the Supreme Court's Management Information Systems Office (MISO) for repair or replacement.

As part of their standard operating procedure, the MISO examined the laptop on 3 January 2020 and found a backup of iPhone messages. After downloading iBackup Viewer, the MISO uncovered a series of messages showing that respondent Judge was engaged in corrupt practices. It then immediately reported the same to the Office of the Court Administrator (OCA), which, on 20 January 2020, hired a private digital forensic expert, Dexter De Laggui (De Laggui) to extract data from the subject laptop and verify the MISO's findings. SMS iMessage conversations, contact



information, photos, videos, and iPhone notes were recovered from the subject laptop.¹⁰

Clearly, Judge Reyes did not transfer or share his data from his mobile phone to a device he owned or purchased in his personal capacity, but to one issued to him by the Court.

This Court has already recognized that employees' expectation of privacy in the workplace may be lawfully limited by the employer monitoring their use of employer-provided computer resources. In *Pollo v. Constantino-David*:¹¹

The CSC in this case had implemented a policy that put its employees on notice that they have no expectation of privacy in anything they create, store, send or receive on the office computers, and that the CSC may monitor the use of the computer resources using both automated or human means. This implies that on-the-spot inspections may be done to ensure that the computer resources were used only for such legitimate business purposes.

One of the factors stated in *O'Connor* which are relevant in determining whether an employee's expectation of privacy in the workplace is reasonable is the existence of a workplace privacy policy. In one case, the US Court of Appeals Eighth Circuit held that a state university employee has not shown that he had a reasonable expectation of privacy in his computer files where the university's computer policy, the computer user is informed not to expect privacy if the university has a legitimate reason to conduct a search. The user is specifically told that computer files, including e-mail, can be searched when the university is responding to a discovery request in the course of litigation. Petitioner employee thus cannot claim a violation of Fourth Amendment rights when university officials conducted a warrantless search of his computer for work-related materials.¹²

Similarly, the National Privacy Commission's Privacy Policy Office has issued Advisory Opinion No. 2018-084 on the monitoring of employees' computers by their employers. To the National Privacy Commission, if the monitoring will entail processing of employees' personal, sensitive personal

¹⁰ *Ponencia*, p. 2.

¹¹ 675 Phil. 225 (2011) [Per J. Villarama, Jr., *En Banc*].

¹² *Id.* at 261-262.

or privileged information,¹³ the processing¹⁴ is allowable under Republic Act No. 10173 if it complies with general data privacy principles. This processing includes the monitoring of employees' activities while they are using office-issued computers:

The [Data Privacy Act] DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Where the computer monitoring results in the collection of personal, sensitive personal or privileged information (collectively, personal data) of employees, the employers are engaged in processing personal data, and thus, covered by the provisions of the DPA.

Monitoring employee activities when he or she is using an office-issued computer may be allowable under the DPA, provided the processing falls under any of the criteria for lawful processing of personal data under Sections 12 and/or 13 of the law.

Employers, as personal information controllers (PICs), shall ensure that the processing complies with the general data privacy principles of transparency, legitimate purpose and proportionality.

First, it is incumbent upon the employer to determine the purpose/s of computer monitoring, which must not be contrary to law, morals, or public policy. Some possible legitimate purposes of computing monitoring are as follows: management of workplace productivity, protection of employees, business assets, intellectual property or other proprietary rights, prevention of vicarious liability where the employer assumes legal responsibility for the actions and behavior of employees, and the like.

Alongside the determination of the purpose of processing, the employer shall assess the proportionality of the information collected, and

¹³ Republic Act No. 10173, sec. 3 distinguishes between these:
SECTION 3. Definition of Terms. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

.....
(g) Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

.....
(k) Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication. ...

(l) Sensitive personal information refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
(4) Specifically established by an executive order or an act of Congress to be kept classified.

¹⁴ "Processing" is defined in Republic Act No. 10173 in Section 3(j), which states:
SECTION 3. Definition of Terms. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

.....
(j) Processing refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

the ways and means of processing. This principle directs the employer to process information that is adequate, relevant, suitable, necessary and not excessive in relation to the declared and specified purpose.

The methodology of data collection should likewise be proportional to the achievement and fulfillment of the purpose of the employer. Thus, personal data of the employees shall only be collected, used and stored by the employer, through computer monitoring, if the purpose sought to be achieved cannot be fulfilled by any other less privacy intrusive means.

In all cases, the employer is duty-bound to inform and notify the data subjects of the nature, purpose, and extent of computer monitoring and processing when using office-issued computers. Moreover, the employer must issue a policy or set of guidelines on the use of company-issued devices and equipment.¹⁵ (Citations omitted)

Specifically, laptops and other personal computing devices issued by this Court to Judiciary officials and personnel are considered information technology resources within the scope of A.M. No. 05-3-08-SC, the Computer Guidelines and Policies of the Supreme Court.¹⁶

SECTION I. PURPOSE

These policies aim to provide general guidelines to all users/employees of the judiciary in using the Information Technology (IT) facilities and resources of the Supreme Court (SC).

.....


SECTION III. SCOPE AND APPLICATION

These policies and guidelines shall apply to all personnel employed by, or contracted by the SC and the Lower Courts (LC), its agencies and offices, including trainees, who are authorized to use IT facilities and resources.

These guidelines cover the proper use of the IT facilities and resources of the Judiciary, which includes but not limited to all IT equipment, software, data in all formats, accessories, networking facilities, and services whether central or remote [including information retrieval services for the public such as web browsing through the worldwide web (www) and file transfer (upload/download)].

For purposes of implementing these policies, any other equipment, computer unit, or external network, when attached to, or used to access and/or interact with any component of the IT facilities and resources of the Court, shall also be considered part of the Court's IT system.

.....



¹⁵ National Privacy Commission Privacy Policy Office Advisory Opinion No. 2018-084, *available at* https://privacy.gov.ph/wp-content/uploads/2022/01/AONo_2018-084.pdf.

¹⁶ A.M. No. 05-3-08-SC, Computer Guidelines and Policies, March 15, 2005.

SECTION V. IT FACILITY AND RESOURCES SECURITY MANAGEMENT UNDER THE MIS OFFICE

The authority and responsibility to install, upgrade or modify any hardware or software rests solely on the MISO and its personnel duly authorized by the chief of MISO.

V.1 The IT facilities and resources

The IT facilities and resources include but are not limited to the following:

1. All cabling used to carry voice and data.
2. All devices to control the flow of voice and data communication, such as hubs, routers, firewalls, switches, and the like,
3. Monitors, storage devices, modems, network cards, memory chips, keyboard, cables and accessories.
4. All computer software including applications, utilities, tools, and databases.
5. All output devices including printers, fax machines, CD writers and similar devices or equipment.

The Computer Guidelines and Policies clearly state that this Court, through its relevant offices particularly the MISO, owns all IT resources enumerated in Section V.1, which are subject to this Court's monitoring:

VI.3 Security Guidelines

Ownership and Right to Monitor. All IT facilities and resources as defined herein are owned by the SC. For this purpose, the Court reserves the right to monitor and/or log all network-based activities. The user shall be responsible to surrender all passwords, files, and/or other required resources it requested to do so, by proper authorities in the presence of his/her office head, or persons authorized by the Court.

....

System Managers/Administrators to Employ Monitoring Tools to Detect improper Use. Electronic communications may be disclosed within an agency or department to employees who have a need to know in the performance of their duties. Agency officials, such as system managers and supervisors, may access any electronic communications.

....

IX.3 No Privacy in Electronic Communications.

Users must never consider electronic communications to be private or secure. E-mail and other electronic communications may be stored indefinitely on any number of computers other than the recipient's.

The Supreme Court reserves the right to monitor and/or log all network-based activities. The user is responsible for surrendering all passwords, files, and/or other required resources if requested to do so in the



presence of his/her Office Head, or persons properly authorized by the Court.

In this regard, the *ponencia* ably distinguishes *Pollo* from another administrative case¹⁷ in which evidence taken from a court employee's personal computer was deemed inadmissible in evidence against him, there being a violation of his right to privacy:

We distinguish *Pollo* from the earlier case of *Anonymous Letter-Complaint against Atty. Miguel Morales, Clerk of Court, Metropolitan Trial Court of Manila (Morales)*, which involves a branch clerk who was investigated based on an anonymous letter alleging that he was consuming his working hours filing and attending to personal cases, using office supplies, equipment, and utilities. The investigating team used the branch clerk's personal computer and printed two documents stored on its hard drive. We emphasize that what is involved in *Morales* was a personal computer, while in *Pollo*, a government-issued computer, hence government property, the use of which the government employer has absolute right to regulate and monitor.¹⁸

To emphasize, the device subject of the unlawful intrusion in *Anonymous Letter-Complaint against Atty. Miguel Morales, Clerk of Court, Metropolitan Trial Court of Manila* was a computer owned by respondent Atty. Morales, which was seized and taken into custody by the Office of the Court Administrator (OCA). This was preceded by a spot investigation by the Deputy Court Administrator and the National Bureau of Investigation¹⁹ without any showing that any search warrant or lawful order authorizing that search and seizure was obtained, or that any of the exceptions to the requirement of a search warrant was present. Those circumstances prompted this Court to find that there was no consented warrantless search of respondent Atty. Morales' personal computer, and the resulting evidence obtained was inadmissible against him.²⁰

In contrast, communications which subjected Judge Reyes to the present administrative proceedings were embodied in data taken not from his personal mobile phone, which presumably remain in his control and possession. No intrusion was made on that particular device. There was also no showing that the MISO, the OCA investigating team, or the judicial audit teams organized by the Court sought to access any copies of Judge Reyes' mobile phone data that may be extant in a cloud data service provider or other off-site storage facility or server. The communications used in evidence in these proceedings came from a copy of the mobile phone data stored in the hard drive of a laptop owned by this Court, paid for with public funds.

¹⁷ *Anonymous Letter-Complaint against Atty. Miguel Morales, Clerk of Court, Metropolitan Trial Court of Manila*, 592 Phil. 102 (2008) [Per J. Austria-Martinez, *En Banc*].

¹⁸ *Ponencia*, p. 29.

¹⁹ *Anonymous Letter-Complaint against Atty. Miguel Morales, Clerk of Court, Metropolitan Trial Court of Manila*, 592 Phil. 102, 107 (2008) [Per J. Austria-Martinez, *En Banc*].

²⁰ *Id.* at 119–121.

When Judge Reyes enabled the synchronization between his Court-issued laptop and his personal iPhone, he did so without being compelled to do so and knowing full well that data from his mobile phone—which may include his digital correspondence with other people, his database of other people’s contact information, photos, and videos²¹—will be stored in that Court-issued laptop. He knew or should have known that the Computer Guidelines and Policies would be applicable to the Court-issued laptop as well as its contents. Any and all data stored on that iPhone which were transferred to the hard drive of the Court-issued laptop thus became subject to regulation and monitoring by this Court.

To preserve the privacy of his personal data, Judge Reyes could have taken measures such as the de-synchronization of his mobile phone and the deletion of his mobile phone data from the Court-issued laptop prior to its reassignment to another judge, but he did not. There was no claim made or evidence presented that the reassignment of the laptop was conducted in a manner that would have reasonably deprived Judge Reyes of the opportunity to remove or destroy any personal information from the laptop that he wished to safekeep, in stark contrast with the spot investigation that took place in *Anonymous Letter-Complaint against Atty. Miguel Morales, Clerk of Court, Metropolitan Trial Court of Manila*. Evidently, he did not value the privacy and security of such data to the extent of taking simple measures that would bolster his claimed defense that he had a reasonable expectation of privacy in his personal mobile phone data stored in the Court-issued laptop.

Thus, this Court correctly does not deem it reasonable to uphold Judge Reyes’ alleged expectation of privacy in his communications in this particular case.

Notably, the Computer Guidelines and Policies further warn the Judiciary that among the prohibited acts in relation to this Court’s Information Technology (IT) resources are uses for personal benefit, business, or partisan activities:

6. Uses for Personal Benefit, Business or Partisan Activities

a. Commercial Use of the IT facility and resources of SC for commercial purposes, and product advertisement, for personal profit, unless allowed under other written Office policies or with the written approval of a competent authority.

b. Use for any partisan activities. Use of IT facility and resources of the SC for religious or political lobbying, for disseminating information or gathering support or

²¹ *Ponencia*, pp. 2, 32.

contributions for social, political or cause-oriented group, which are inconsistent with the activities of the Court.

It was reasonable for MISO in this case to have examined the data that was stored in the Court-issued laptop in order to reasonably ascertain whether or not this particular IT resource had been used to do any of the prohibited acts enumerated in the Computer Guidelines and Policies, including the use of the laptop for personal benefit or business, or even simply to ascertain if that data should be preserved as part of judicial data records. Being a reasonable search of a Court-owned IT resource, it follows that the evidence obtained as a result of this search is not subject of the exclusionary rule articulated in our Constitution.²²

Likewise, I agree with the *ponencia* that the information obtained by the judicial audit teams are also not covered by exclusionary rule.²³

ACCORDINGLY, I vote to find Judge Edralin C. Reyes, Presiding Judge, Branch 43, Regional Trial Court of Roxas City, Oriental Mindoro administratively **GUILTY** of gross misconduct and simple misconduct.



MARVIC M.V.F. LEONEN
Senior Associate Justice

²² CONST., art. 3, sec. 3 states:

SECTION 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

(2) Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.

²³ *Ponencia*, pp. 32-33.