I. INTRODUCTION

The current Philippine workplace is the subject of massive technological advances and innovative pieces of legislation designed to protect an individual's privacy. "This technology is both a blessing and a curse in the employment arena. Sophisticated monitoring software and hardware allow businesses to conduct basic business transactions, avoid liability, conduct investigations and, ultimately, achieve success in a competitive global environment. Employees can also benefit when monitoring provides immediate feedback, keeps the workforce efficient and focused and discourages unethical/illegal behavior. The same technology, however, allows employers to monitor every detail of their employees' actions, communications and whereabouts both inside and outside the workplace. As more and more employers conduct some form of monitoring, the practice will shortly become ubiquitous. This trend is problematic because excessive and unreasonable monitoring can: (1) invade an employee's reasonable expectation of privacy, (2) lead employees to sneak around to conduct personal activities on work time, (3) lower morale, (4) cause employees to complain and, potentially, quit and (5) cause employees to fear using equipment even for benign work purposes."[1]

Employers, in their attempt to maximize efficiency and productivity may resort to more extensive monitoring of employee activities within the workplace. "An increasing number of employers are electronically monitoring their employees' use of email, the Internet, telephones, and computers. This increased monitoring has fuelled concern about the conflict between employers' rights to protect their business and property, and employees' right to privacy."[2]

While the 1987 Constitution recognizes the employers' management prerogative, new legislation was enacted by Congress that seek to regulate the gathering and use of private data to protect an individual's right to privacy.

At present, the rules on the use of private data disclosed and, or gathered during the course of one's employment are not clearly defined. Thus, it is not far-fetched for employers to monitor and record an employee's conduct or behaviour through electronic eavesdropping. This kind of activity by the employers will definitely give rise to privacy issues.

Is the information on the employee gathered through electronic monitoring or contemporary monitoring techniques not contrary to the employee's right to privacy? If other entities request for information on a prospective employee from the previous employer, is it considered as personal information which requires prior consent of the employee for its release?

This paper seeks to identify the applicable laws and rules, and will present possible answers to the above-stated questions.

---

[1] *THE EAVESDROPPING EMPLOYER: A TWENTY-FIRST CENTURY FRAMEWORK FOR EMPLOYEE MONITORING, Corey A. Ciocchetti, http://www.futureofprivacy.org/wp-content/uploads/2010/07, page 1.*

[2] *Privacy at Work, Mahak Nayar, David Thaw, Erin Straughan, Cynthia Owens http://www.gvpt.umd.edu, page 1.*

II. MANAGEMENT PREROGATIVE: A SPECIES OF PRIVATE ENTERPRISE SYSTEM

Employers' extensive use of different monitoring methods may be justified as a management prerogative. Management prerogative is a species of the private enterprise system which is recognized by the 1987 Constitution. It provides that, "the State recognizes the indispensable role of the private sector, encourages private enterprises, and provides incentives to needed investments. The State is mandated to regulate the relations between workers and employers. While labor is entitled to a just share in the fruits of production, the enterprise has an equally important right not only to reasonable returns on investments but also to expansion and growth.[3]

"Neither the 1987 Constitution nor the Labor Code which took effect in 1974, defines private enterprise, but in 1994, a legislative definition was formally stated in R.A. No. 7796, the TESDA Law, which seeks active participation of private enterprises in providing and developing technical education and skills. 'Private enterprises,' Section 4 of the TESDA Law says, is an 'economic system under which property of all kinds can be privately owned and in which individuals, alone or in association with another, can embark on a business activity. This includes industrial, agricultural, or agro-industrial establishments engaged in the production, manufacturing, processing, repacking or assembly of goods including service-oriented enterprises.' This definition is applicable to private business operations, in general, throughout the country."[4]

While the 1987 Constitution promotes social justice by protecting the working class, it also recognizes the rights of the employers. "Management also has its own rights which are entitled to respect and enforcement in the interest of fair play."[5] "Management prerogative, however, are subject to limitations provided by (1) law, (2) contract or collective bargaining agreements, and (3) general principles of fair play and justice."[6]

"Briefly introduced below are the most fundamental of the management rights:

> "Right to ROI. The employer has the right to return of investments and to make profit. There is nothing dirty about profit per se- it is profit that creates jobs and improves the workers' lot.
>
> "Right to Prescribe Rules. Employers have the right to make reasonable rules and regulations for the government of their employees, and when employees, with knowledge of an established rule, enter the services, the rule becomes a part of the contract of employment. Company policies and regulations are, unless shown to

---

[3] *The Labor Code with Comments and Case, Volume 1, C.A. Azucena, Jr., Rex Bookstore, Manila, Philippines, page 14.*
[4] *Ibid.*
[5] *Ibid. page 28.*
[6] *Gelmart Industries, Phils., Inc., vs. NLRC, G.R. No. 55668, August 10, 1989.*

be grossly oppressive or contrary to law, generally binding and valid on the parties.

> "Right to Select Employees. An employer has a right to select his employees and to decided when to engage them. He has a right under the law to full freedom in employing any person free to accept employment from him and this, except as restricted by valid statute or valid contract, at a wage and under conditions agreeable to them. On the one hand, he may refuse to employ whomever he may wish, irrespective of this motive, and on the other hand, he has the right to prescribe the terms upon which he will consent to the relationship, and to have them fairly understood and expressed in advance. The state has no right to interfere in a private employment and stipulate the terms of the services to be rendered; it cannot interfere with the liberty of contract with respect to labor except in the exercise of police power.
>
> "Right to Transfer or Discharge Employees. An employer has he perfect right to transfer, reduce or lay-off personnel in order to minimize expenses and to insure the stability of the business and even close the business. This right to transfer of discharge has been consistently upheld even in the present era of multifarious reforms in the relationship of capital and labor, provided the transfer or dismissal is not abused but in good faith and in due to causes beyond control. To hold otherwise would be oppressive and inhuman."[7]

In *Julies Bakeshop and/or Edgar Reyes vs. Henry Arnaiz, Edgar Napal, and Jonathan Tolores*[8], the Supreme Court held:

> We have held that management is free to regulate, according to its own discretion and judgment, all aspects of employment, including hiring, work assignments, working methods, time, place and manner of work, processes to be followed, supervision of workers, working regulations, transfer of employees, work supervision, lay off of workers and discipline, dismissal and recall of workers. The exercise of management prerogative, however, is not absolute as it must be exercised in good faith and with due regard to the rights of labor.

In case of a conflict between the employer's management prerogative and an employee's rights, for as long as the management action was done in good faith and not contrary to law, such exercise is considered valid. In *Dannie M. Pantoja vs. SCA Hygeine Products Corporation*[9], the Supreme Court, declared:

> Once again, we uphold the employer's exercise of its management prerogative because it was done for the advancement of its interest and not for the purpose of defeating the lawful rights of an employee.

---

[7] *The Labor Code with Comments and Case, Ibid. pages 29 to 30.*
[8] *G.R. No. 173882, February 15, 2012.*
[9] *G.R. No. 163554, April 23, 2010.*

Thus, electronic eavesdropping on an employee may be a valid exercise of the employer's management prerogative. It may fall within the right to prescribe rules and the right to discharge employees. The employer may set rules as regards the use of computers and the company network. The employer shall then monitor the employee's behaviour and work performance based on the use and access of the company computer and network. The employee's behaviour and work performance will be used as an indicator of his fitness to remain engaged or to be discharged if it constitute grounds for termination under the company rules and, or Article 296 [282][10] of the Labor Code.

Employers may have various reasons why they resort to electronic monitoring. "According to a 2001 survey conducted by the American Management Association, "more than three-quarters (77.7%) of major U.S. firms record and review employee communications and activities on the job, including email, Internet connections and computer files. This percentage has increased twofold since 1997. Reasons for increased monitoring are related to the increased access to the Internet and email employees have now in the workplace. Other reasons noted by companies who did monitor their employees included:

1. Legal compliance—industries such as telemarketing which needed to record to protect both the company and the consumer if legal issues do arise, and for the company's "due diligence" to maintain correct records;
2. Legal liability—to protect the company against suits from employees who are unwillingly subject to hostile or pornographic materials and might in turn bring charges against the company for a hostile workplace;
3. Performance review—so employers can make sure the work is getting done to a satisfactory level, and to be used for employees that might be on contracts that go up for review in a certain number of years;
4. Productivity measures—to make sure the employees are not abusing the Internet or email on designated work time, and
5. Security reasons—to make sure the company's information is being protected and that certain copyright laws are not being violated

Generally, employers that do monitor employees tend to think that if employees know that they are being watched or monitored some of the time, this will

---

[10] *Termination by employer. - An employer may terminate an employment for any of the following causes:*

(a) Serious misconduct or willful disobedience by the employee of the lawful orders of his employer or representative in connection with his work;

(b) Gross and habitual neglect by the employee of his duties;

(c) Fraud or willful breach by the employee of the trust reposed in him by his employer or duly authorized representative; c

(d) Commission of a crime or offense by the employee against the person of his employer or any immediate member of his family or his duly authorized representatives; and

(e) Other causes analogous to the foregoing.

help prevent any misconduct from potentially happening in the first place and will increase productivity."

Thus, electronic monitoring may be justified under "the general philosophy that: (1) workplaces exist for work purposes, (2) employers provide technology and pay wages in return for performance and (3) liability issues override the instinct to enhance employee privacy interests. This philosophy has merit and comprises the most rational and workable foundation for an employee monitoring regime. This is especially true under the doctrine of employment at will which is an implicit agreement between employers and employees that employees may be fired for any legal reason."[11]

As earlier stated, the advances in technology enabled "employers have taken a multitude of approaches and monitor their employees in many different ways. For the most part, this monitoring takes place inside the workplace. However, monitoring may also occur outside of the workplace (i.e., GPS tracking of company vehicles or remote e-mail monitoring) or outside of the employment relationship (i.e., investigation of an employee's gambling habits)."[12]

"Contemporary monitoring techniques include:

a. ACCESS PANELS;
b. ATTENDANCE & TIME MONITORING;
c. AUTOMATIC SCREEN WARNINGS;
d. DESKTOP MONITORING;
e. E-MAIL & TEXT MESSAGE MONITORING;
f. FILTERS & FIREWALLS;
g. GPS & RFID MONITORING;
h. INTERNET & CLICKSTREAM DATA MONITORING;
i. KEYSTROKE MONITORING;
j. PHYSICAL SEARCHES;
k. SOCIAL NETWORK & SEARCH ENGINE MONITORING;
l. TELEPHONE & VOICEMAIL MONITORING;
m. VIDEO SURVEILLANCE"[13]

"Access Panels are electronic devices programmed to control entry into a doorway, stairwell, elevator, parking garage, or other restricted area. Typical panels require employees to enter a password, provide a fingerprint/iris scan, or swipe an identification card. Authorized credentials are logged in the system as the panel electronically unlocks the passageway. Unauthorized entry attempts also create a log record and can sound a silent or audible alarm to alert company personnel and/or law enforcement."[14]

"As regards time and attendance monitoring, it is an understatement to claim that attendance is a key component of workplace productivity. Workers who fail to

[11] *The Eavesdropping Employer, Ibid. page 9.*
[12] *Id. Page 18.*
[13] *Ibid., page 19.*
[14] *Id.*

show up on time, leave early or miss extended amounts of time are also liabilities from a monetary and legal standpoint. It is more efficient to monitor employee hours via software as opposed to on paper as it reduces hours inflation and human errors. Attendance software is programmed to monitor attendance patterns and trends to determine which employees may be excessively absent or taking advantage of the system. This software can cross-reference employee attendance rates across department and alert employers to problem areas. Employers can be required to enter the reason behind their absence which can help employers implement solutions."[15]

"Automatic Screen Warnings are disclaimers which load automatically onto employee screens before the system grants access to the requested program. These warnings are intended to inform employees that they are being or may be monitored. Such screens can be customized to list each item that the employer monitors or employers can limit the disclosure to the monitoring about to take place. Automatic screen warnings can be an important for compliance with a company policy that promises to disclose monitoring practices before they take place. It is important to note that automatic screen warnings are not required before monitoring takes place. In fact, one court has held that employers who breach their promises not to monitor without such notice may still do so without violating any employees' right to privacy. The prudent course, however, is to adhere to such promises or not make them at all. Such notice will help defeat any reasonable expectation of privacy an employee has in any given electronic activity."[16]

"Desktop monitoring programs can obtain every command and keystroke sent to the desktop by a user, translate these signals into data and remotely transmit this information to the employer. Desktop monitoring programs can be installed physically or remotely via a "trojan horse" e-mail attachment. These programs can record and copy, in real-time, the following activities which occur on an employee's desktop:

1. **APPLICATION TRACKING** - tracks which software applications are used and for how long;
2. **DOCUMENT TRACKING** - tracks each document accessed on an individual computer;
3. **EVENTS TIMELINE** - tracks the order in which employees work on assignments;
4. **LOG-ON MONITORING** - tracks how often and when employees log-on to employer's system;
5. **PASSWORD LOGGING** - tracks any passwords entered over the employee's computer;
6. **PRINT JOBS EXECUTED** - tracks individual print requests;
7. **SCREENSHOT CAPTURE** - tracks information on an employee's screen at any given time;
8. **SOFTWARE INSTALLATION** - tracks any software loaded onto an employee's computer; and

---

[15] *Id., pages 20 to 21.*
[16] *Id., pages 22 to 23.*

9. **WINDOW ACTIVITY** - tracks all windows opened per session."[17]

"Monitoring e-mail accounts is a common practice and over 40% of all employers monitor at least a portion of their employee e-mail accounts. This form of monitoring is generally implemented via software programs capable of tracking the content, timing, volume and recipients of sent and received email. These sophisticated programs can even track an employee's Web-based e-mail accounts provided by, for example, America Online, Hotmail or Yahoo - personal accounts that employees often assume are off-limits to monitoring. The extent of such tracking is large in scope as over 60 million employees have e-mail and/or Internet access at work.85 96% of employers who monitor e-mail track external - incoming and outgoing - e-mails. Employers monitor their employees' e-mail for a multitude of reasons, the most important being to: (1) check in on productivity, (2) look for sexual harassment/sex discrimination and workplace violence (3) look for offensive language and/or pornography and (4) monitor language for transmission of trade secrets or other confidential information. Such monitoring can help lower legal liability."[18]

"Filters and firewalls not only prevent outsiders from gaining access to an employer's system - they also can be used to prevent employees from accessing information or Web sites unrelated to work. This firewall is designed to make employees more productive and stop non-work related activities during work hours. To this end, 65% of employers block unauthorized or inappropriate Web sites on employee computers. The vast majority of such filters block Web sites categorized as adult with "sexual, romantic [and/or] pornographic content." Filters also block Web sites dedicated to gaming, social networking, entertainment, shopping and sports. 18% of employers filter out external blogs as well. The effectiveness of this monitoring program can be questioned as most employees can access prohibited sites from their personal PDA or smartphone thereby circumventing the employer's firewalls and filters."[19]

"Global Positioning Systems (GPS) and Radio Frequency Identification Devices (RFID) are electronic tracking devices. This technology provides precise location information of objects or individuals on a real-time basis by triangulating satellite signals. Employers utilize these tracking devices to monitor the whereabouts of their employees and property. It is important to note that GPS and RFID devices are not solely designed to monitor vehicles; these devices often monitor employee cell phones, laptops, PDAs and Smartcards or other forms of employer property. Employers also use this technology to authorize the operation of equipment, track their employees' location within the workplace, and even determine if employees are working the amount of hours claimed on time sheets. This technology can also be used to produce real-time reports on employee productivity and encourage competition among employees to be more productive."[20]

---

[17] *Id., page 23.*
[18] *Id., page 24.*
[19] *Id., page 25.*
[20] *Id.*

"Otherwise known as Internet monitoring, Internet Use Audits track an employee's Web activity over a period of time. Employers utilize this technology to determine employee productivity and to check for inappropriate activities. 30% of employers have terminated an employee for unauthorized Internet use. 84% of such terminations were at least partially based on an employee's viewing or downloading inappropriate and/or offensive content. Internet Use Audits can be minimal, moderate or all-encompassing. Minimal audits occur when employers collect anonymous data on which Web sites their employees view. These reports may be used to set or amend current Internet Use policies. Moderate audits are a bit more intrusive and analyse specific Web sites visited by individual employees during work hours. All-encompassing Internet Use Audits occur when employers collect and mine clickstream data. Clickstream data are the "electronic footprints created when a Web user moves about in cyberspace." Clickstream technology records each mouse click on each Web page visited as a user navigates the World Wide Web. Clickstream data can be "shockingly revealing, providing a record of the entirety of one's online experience, including movements among Web sites, geographical location, the type of computer and Internet browser in use, and any transactions or comments made at individual Web sites." Clickstream monitoring allows employers to accurately recreate entire periods (i.e., specific days, quarters, projects) and determine employee productivity, focus and adherence to company policy."[21]

"Also called key-logging, this form of monitoring occurs when individual key strokes are recorded/logged and made accessible to others. Logging occurs via a hardware device physically attached to the user's computer or a software program installed on a user's computer. Logging programs allow employers to enter a password and convert keyboard-based activities into text. These results are used to determine employee effectiveness and productivity. As with most types of employee monitoring keystroke logging is generally done in secret to obtain more accurate results."[22]

"Employment-related searches are one of the oldest forms of employee monitoring. Through such searches, employers generally seek to monitor employees for illegal drug use, theft, or the possession of alcohol or weapons.137 A lesser known form of physical searches is referred to as dumpster diving. Dumpster diving is a rather drastic form of employee monitoring. This occurs when employers physically search through employee's trash and recycling looking for information. Oftentimes employees merely discard documents without shredding them. This allows an employer, with access to employee offices, to re-create an accurate record of employee actions in the workplace. The law allows employers to retain access to all areas of their workplace - even if they provide individual employees with personal offices and vehicles. Employers have the right to enter these offices and conduct searches almost at any time. The only places that remain off-limits are those where employees retain a "reasonable expectation of privacy." Such an expectation is common in personal belongings stored in offices (i.e, purses or wallets) and potentially locked desk drawers. Some employers have chosen to physically search employee vehicles. Random searches - even if included in a policy - are frowned

[21] *Id., page 27.*
[22] *Id., page 29.*

upon. Physical searches involving personal items such as briefcases/wallets/purses or of an employee's body are likely invasions of an employee's reasonable expectation of privacy."[23]

"Social Networking and Search Engine monitoring is one of the most recent forms of employee monitoring. It is also one of the cheapest. All an employer needs is an Internet connection, a browser and basic knowledge of how such programs operate. Social-networking monitoring involves creating an account on a Web site such as Facebook or MySpace and then searching the name of the employee/applicant. A treasure trove of information may appear at the click of a mouse as these sites make it easy to upload incriminating pictures, post silly or discriminatory quotations and identify known associates (i.e., friends). Unless the user sets the privacy setting to "Friends Only," their profile is freely available to anyone who searches. In fact, employees are becoming more conscious of just how easy this form of monitoring has become. 29% of employees have become more conservative online because they fear that "employers can use anything and everything as an excuse to fire" them in a down economy. Search engine monitoring is just as simple as social-network monitoring. To conduct these searches, an employer merely requests the search engine homepage (such as Google.com or Yahoo.com) and searches for the employee's/applicant's name. Within seconds (Google even keeps track of the time it takes to complete the search) potentially hundreds of links appear. Most of the time the person's name appears somewhere within the Web page targeted by the link. Employees need only sit back and discover a great deal of potentially embarrassing information. It is much easier to find juicy information about an employee on social networking sites because that is one of their major points of existence. However, conducting a Google search has some advantages over a Facebook search. First, individual's cannot make their name private from search. Indeed, it is very difficult to force a search engine to remove even one link an individual considers inappropriate. Second, employees do not need as much instruction on how to conduct a search engine inquiry as they do to navigate MySpace for information. In the end, both social-networking and search engine inquiries are legal, efficient, inexpensive and powerful monitoring tools."[24]

"Telephone monitoring tracks the amount of time spent on calls, phone numbers dialled, breaks between receiving calls, etc. Employers are looking for theft of trade secrets and confidential information, violence between co-workers or an employee and a customer, sabotage and performance issues. Merely monitoring telephone calls likely does not create major legal problems. Federal law and most state laws allow monitoring as long as one party to the conversation consents. With this in mind, companies create telephone monitoring consent policies satisfying this requirement. Voicemail monitoring allows employers to listen to employee voicemail in order to determine the same issues as are relevant in telephone monitoring. Contemporary voicemail programs can monitor messages using a "Unified Messaging" program that turns voicemail into audio files and e-mail text. Finally, text messages are fast becoming the preferred method of communication. Text messages are composed and sent via cell phone to recipients from the user's contacts list.

[23] *Id., page 31.*
[24] *Id., page 32.*

Employees are much more likely to monitor text messages sent from employer-provided equipment than from employee's personal cell phones."[25]

"Video surveillance involves the taping of employees within workplace facilities or outside of the workplace conducting work activities.150 In lieu of software desktop, e-mail or Internet monitoring, employers can point a video camera directly at computer screens to monitor computer-based activity. In a 2007 survey by the American Management Association, 47% of employers admitted to monitoring their employees via this method - up from just over 30% in 2001. Just under 50% of those admitting to monitoring claimed that video surveillance is ongoing as opposed to routine, occasional or specific. Video surveillance is primarily intended to:

1. Increase safety of employees (by decreasing violence and threatening behavior and locating workplace risks);
2. Discourage drug/alcohol use, theft or sabotage and otherwise protect employer property; and/ or
3. Monitor employee productivity.

Some employers place hidden cameras throughout the workplace while others are purposefully overt. Hidden cameras provide the element of surprise and are likely to capture more accurate results. Overt cameras, on the other hand, are placed in public view to discourage bad behaviour and to encourage productivity. Other employers place fake or deactivated cameras in the workplace to gain the advantage of overt surveillance without the cost of actual cameras. Finally, it is important to remember that employer-owed video surveillance equipment can be misused by employees which may lead to sexual harassment or invasion of privacy lawsuits. Over 70% of employers who conduct video surveillance notify their employees beforehand."[26]

III. DATA PRIVACY ACT OF 2012

REPUBLIC ACT NO. 10173, **"***AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES*", otherwise known as "Data Privacy Act of 2012" protects[27] the "personal information" in the information and communications systems in the government or in the private sector.

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."[28]

---

[25] *Id., page 33.*
[26] *Id., page 34.*
[27] *SEC. 2.* Declaration of Policy. – *It is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.*
[28] *Section 3(g) R.A. No.10173.*

Sensitive Personal Information[29] 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 cm-rent 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.

Data subject refers to an individual whose personal information is processed.[30] The *personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes: (1) A person or organization who performs such functions as instructed by another person or organization; and (2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.[31] In a work environment, the data subject is the employee and the personal information controller is the employer.

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.[32] Thus, the above-stated contemporary monitoring techniques clearly fall under the act of "processing".

"The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

"Personal information must, be:

---

[29] *Section 3(l), Id.*

[30] *Section 3. (c), Id.*
[31] *Section 3. (h), Id.*

[32] *Section 3. (j), Id.*

"(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;

"(b) Processed fairly and lawfully;

"(c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

"(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(e) Retained only for as long as necessary for the fulfilment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

"(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.

"The personal information controller must ensure implementation of personal information processing principles set out herein."[33]

The law further requires that "the processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:

"(a) The data subject has given his or her consent;

"(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

"(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

"(d) The processing is necessary to protect vitally important interests of the data subject, including life and health;

[33] *Sec. 11, Id.*

> "(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> "(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution."[34]

When the personal information is sensitive personal information, the law imposes stricter requirement before it may be processed. In fact, processing of "sensitive personal information and privileged information shall be prohibited, except in the following cases:

> "(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
>
> "(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
>
> "(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
>
> "(d) The processing is necessary to achieve the lawful and non-commercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing;
>
> "(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

[34] *Sec. 12., Id.*

> "(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority."[35]

Thus, for the employer to perform any of the above-acts of contemporary monitoring techniques there must be compliance with Section 11, 12 and 13 of R.A. No. 10173. Also, before any information will be disclosed by the data subject, the law requires that the data subject must be notified that the information he will disclose will be processed. However, when the disclosure of personal information by the data subject to a personal information controller is made within the context of an employer-employee relationship[36], the latter is not required to give the required notice to the data subject.

From a broader perspective, an employee's conduct in the workplace which will be recorded through the various monitoring techniques may be considered as personal information, as such data will provide the identity of an individual or, from which the identity of an individual may be directly or reasonably ascertained. This kind of personal information is not disclosed to the employer directly and voluntarily, rather, it is deduced after data is processed through contemporary monitoring techniques. If the data gathered constitute sensitive personal information or privileged information[37], the employer practically violates paragraph (c) of Section 13.

---

[35] *Sec. 13, Id.*

[36] SEC. 16. *Rights of the Data Subject. xxx* (b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity: xxx xxx

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided,* That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a *subpoena* or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

[37] *Rules of Court, Rule 130,* ***Section 24.*** *Disqualification by reason of privileged communication. — The following persons cannot testify as to matters learned in confidence in the following cases:*

> *(a) The husband or the wife, during or after the marriage, cannot be examined without the consent of the other as to any communication received in confidence by one from the other during the marriage except in a civil case by one against the other, or in a criminal case for a crime committed by one against the other or the latter's direct descendants or ascendants;*
>
> *(b) An attorney cannot, without the consent of his client, be examined as to any communication made by the client to him, or his advice given thereon in the course of, or with a view to, professional employment, nor can an attorney's secretary, stenographer, or clerk be examined, without the consent of the client and his employer, concerning any fact the knowledge of which has been acquired in such capacity;*

As earlier propositioned, the use of contemporary monitoring techniques by the employer may be valid if exercised as a management prerogative. However, in the course of processing the information, if sensitive personal information or privileged information is discovered, the employer may be liable for violation of Section 13, paragraph (c) as the law absolutely requires the consent of the employee "specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing".

Another issue is the disclosure of information processed through contemporary monitoring techniques to third parties. Human resource departments of companies usually conduct background checks of an applicant's employment history. It is not unusual for employers to provide information as regards date of hiring and position. They may even go to the extent of providing the previous employee's job description. There are also those who inquire into the employee's performance rating and if the employee had prior violations of company rules. All these information do not originate from the employee but processed by the employer in the course of the employment of the employee. Thus, there is no requirement of prior notice as required by Section 13. While prior notice may be dispensed with, processing of personal information by third parties not falling under Section 12 and 13 is clearly a violation of the personal information controller.

IV. CONCLUSION

The use of electronic monitoring or contemporary monitoring techniques by employers in the Philippine workplace may soon be a standard. The use of such monitoring techniques is valid if exercised as a management prerogative. To protect an employee's right to privacy, a rule must be promulgated to require employers to post clear and apparent notices or warnings within the wokplace to the employees that they are subjected to monitoring. In fact, Section 16 should be amended to delete the exception to prior notice if the information is disclosed or processed in the context of employer-employee relationship.

The Department of Labor and Employment must promulgate rules on the use electronic monitoring by employers. The department must provide a list of contemporary monitoring techniques that will be allowed within the workplace. It

---

(c) A person authorized to practice medicine, surgery or obstetrics cannot in a civil case, without the consent of the patient, be examined as to any advice or treatment given by him or any information which he may have acquired in attending such patient in a professional capacity, which information was necessary to enable him to act in capacity, and which would blacken the reputation of the patient;

(d) A minister or priest cannot, without the consent of the person making the confession, be examined as to any confession made to or any advice given by him in his professional character in the course of discipline enjoined by the church to which the minister or priest belongs;

(e) A public officer cannot be examined during his term of office or afterwards, as to communications made to him in official confidence, when the court finds that the public interest would suffer by the disclosure.

should also provide for safety mechanisms to ensure the protection of the employee's right to privacy.