# Labor Relations and the E-Commerce Act of 2000

MARCIAL G. DE LA FUENTE*

On 14 June 2000 Republic Act 8792 was signed into law. The Electronic Commerce Act of 2000 was the Philippine government's response to the rapid development of information and communication technology (ICT), which was anticipated to influence the conduct of business in the country in much the same way that it has done in technologically advanced societies.

This paper is a discussion of the potential effects of the passage of this law on labor relations.

## Electronic contracting and labor relations

When an applicant has already been offered the job he applied for, the first step to integrate him with the employer company is, of course, the execution and signing of an employment contract. In the course of his employment, he may enter into several other contracts or agreements with the company such as training agreements, an agreement for the acquisition of a car, etc. Obviously, as it is being practiced today, the employee must appear and personally sign the contract or agreement.

Under the New Civil Code, while a contract is perfected by the meeting of minds between the parties to it[1] and a contract shall be obligatory in whatever form it may have been entered into,[2] there are certain agreements which must be in writing; otherwise, they would either be invalid or unenforceable. Examples are listed under Article 1403 of the Civil Code. If an agreement covered by Article 1403 is entered into between the employer and the employee or is incorporated in the

* *ACCRA Law Office*

[1] Article 1305.
[2] Article 1356.

*Philippine Journal of Labor & Industrial Relations, vol. xix-xx (1999-2000): 75-88*

employment contract, the same must, therefore, be in writing for it to be enforceable. Apparently, "writing" refers to something that is reduced to paper or similar form.

With the advent of electronic transactions, however, parties may sometimes dispense with copies of agreements or contracts and use diskettes or hard drives instead. It appears that our Civil Code provisions do not cover electronic transactions or contracting. The E-Commerce Act is the fitting response to such a problem.

Section 16, Chapter III of the Act provides that:

> [E]xcept as otherwise agreed by the parties, an offer, the acceptance of an offer and such other elements required under existing laws for the formation and perfection of contracts may be expressed in, demonstrated and proved by means of electronic data messages or electronic documents, and no contract shall be denied validity or enforceability on the sole ground that it is in the form of an electronic data message or electronic document, or that any or all of the elements required under existing laws for the formation of the contracts [are] expressed, demonstrated and proved by means of electronic data messages or electronic documents.

Section 17 of the same chapter provides:

> As between the originator and the addressee of an electronic data message or electronic document, a declaration of will or other statement shall not be denied legal effect, validity or enforceability on the ground that it is in the form of an electronic data message or electronic document.

As the Act allows electronic contracting, such contracts or agreements as employment, service, consultancy, and training between a company and its employees and/or another company may now be entered into by merely clicking the computer's keyboard or mouse. The presence of the parties at a particular place and at a particular time may now be dispensed with, thus saving substantial work time. It appears now that the medium in which a contract or document is created does not affect its legal significance. Be that as it may, we should consider also the so-called "click-wrap" contracts. It must not be considered as a hard and fast rule that, since the Act allows electronic contracts, then all such contracts would be considered as valid. It may happen that an employee does not anymore possess the bargaining power and may yet click the "I accept" button to "perfect" the contract. In such a case, our courts may strike the contract down for being a contract of adhesion where one of the contracting parties possesses no bargaining power.

## Evidentiary issues and problems

The dissemination of information, through memoranda and notices, to the employees is facilitated with the use of an intranet system in the Company. However, problems may arise with respect to, among others, the binding effects of such notices or memoranda, especially if the employees deny having received them through their computers.

This is especially true with respect to an employee who has been charged and investigated for an offense and who consequently files a case for illegal dismissal. In the prosecution of the case, evidentiary issues will surely arise.

Under the Labor Code, as amended, before an employee may be dismissed, there must be compliance with both substantive and procedural due process. Substantive due process is complied with if the termination is based on either a just or authorized cause as provided under the Labor Code, as amended. Procedural due process requires that (1) the employee must be notified of the charges against him; (2) he must be given the opportunity to be heard; and (3) he must be given a notice of termination whereby the reasons for his dismissal are explained. The employee may opt to exercise his right to be heard by submitting a written reply to the charges against him.

It is easy to comply with the two-notice requirement if we follow the present practice of giving the employee the said notices in paper or hard copy form. This is also true with respect to the written reply. Evidence of delivery and receipt would not be a problem as the paper itself would be the best proof of such service and receipt. Identification and authentication would not be a problem either.

The Act, however, allows the use and transmission of electronic data message or electronic document. As defined in the Act, electronic data message refers to information generated, sent, received or stored by electronic, optical or similar means; and electronic document refers to information or the representation of information, data, figures, symbols or other modes of written statement, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.

If the notices and the reply, for instance, are sent and received through the e-mail, problems may arise if the employee or the employer, as the case maybe, would deny having received the same. The employee can always contend that he was not apprised of the charge against him as he never received the e-mail. The employer, on the other hand, may

construe the absence of a written reply as an admission of guilt and proceed to dismiss the employee.

The additional problem arises of how to present the electronic document and have it admitted in evidence before the labor tribunals. A printout offered in evidence might have to be supported by presentation of the digital version. Will a diskette file suffice for the purpose, or should the tribunal be given access to the whole computer system in which the document is lodged? There is, of course, the necessity of authenticating the paper and digital versions.

In other words, the integrity, reliability and authenticity of the electronic documents are bound to be problematic. Proof of service and receipt would also be an issue.

A careful perusal of our present rules of evidence show that they are not adequate to deal with simple computer-generated printouts. There is no reference therein to computer printouts as evidence. Thus, it can be said that our rules likewise cannot offer solutions to issues raised by the introduction of new electronic documents or data messages where there are no "writings" to speak of.

It is assumed, however, that with the enactment of the E-Commerce Act, the evidentiary issues and problems brought about by the information technology revolution will be properly addressed.

The E-Commerce Act grants legal recognition to electronic data messages and electronic documents and provides that they shall not be denied validity or enforceability on the sole ground that they are in electronic form. Further, it is declared that "for evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws."[3]

The burden is on the person seeking to introduce an electronic data message and electronic document in any legal proceeding to prove the authenticity of the document by evidence capable of supporting a finding that the electronic data message and electronic document is what he claims it to be.[4] To sustain the proponent's burden, he must show the origin and prove the integrity of the electronic data message or document.

Under the E-Commerce Act, authentication is facilitated by the presence of an electronic signature on the document. Section 8 of the Act provides that "an electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if the signature is an electronic signature and proved by showing that a

[3] Section 7.
[4] Sec. 11.

prescribed procedure, not alterable by the parties in the electronic document, existed."

The problem regarding the service and receipt of the notices and written reply or explanation is addressed by Sections 18 to 23 of the Act.

The case of *IBM Philippines, Inc. v. NLRC*[5] preceded the E-Commerce Act but may serve as an illustration of the evidentiary matters we have considered. The case arose out of the termination of an employee of petitioner IBM Philippines, Inc. on grounds of habitual tardiness and absenteeism. The dismissed employee contended that he was summarily dismissed and was not given an opportunity to air his side on the matter. Petitioner alleged that the employee was constantly told of his poor attendance record and inefficiency through the company's internal electronic mail (e-mail). According to petitioner, this system allows paperless or "telematic" communication among IBM personnel in the company's offices here and abroad. An employee is assigned a "User ID" and the corresponding password is provided by the employee himself and, theoretically, known only to him. Employees are then expected to turn on their computers everyday, "log in" to the system by keying in their respective IDs and passwords in order to access and read the messages sent to and stored in the computer system. To reply, an employee types in or encodes his message-response and sends the same to the intended recipient, also via the computer system. The system automatically records the time and date each message was sent and received, including the identification of the sender and receiver.

Petitioner attached copies of the printouts of the e-mail messages to its position paper and sought to have these admitted as evidence. Through the computer printouts calling the employee's attention to his alleged tardiness and absenteeism, petitioner sought to prove that the employee was sufficiently notified of the charges against him and was guilty of such charges because of his failure to deny the same.

Before the Supreme Court, the petitioner argued that the computer printouts submitted by them need not be authenticated according to the rules of procedure in regular courts in order that these may be admitted as evidence. They based their argument on the rule that administrative agencies need not be bound by the technical rules of procedure and evidence in disposing of cases before such bodies. The Supreme Court agreed that such was the rule, but subject to the limitation

[5] 305 SCRA 592 (1999).

of the basic evidentiary rule that the evidence presented must at least have a modicum of admissibility to be given some probative value.[6]

The Supreme Court then ruled, thus:

> **The computer print-outs**, which constitute the only evidence of petitioners, **afford no assurance of their authenticity because they are unsigned**. The decisions of this Court, while adhering to a liberal view in the conduct of proceedings before administrative agencies, have nonetheless consistently required some proof of authenticity or reliability as condition for the admission of documents.[7]
>
> x x x
>
> Not one of the 18 print-out copies submitted by petitioners was ever signed, either by the sender or the receiver. There is thus no guarantee that the message sent was the same message received. As the Solicitor General pointed out, the messages were transmitted to and received not by the private respondent himself but his computer.
>
> **Neither were the computer print-outs certified or authenticated by any company official who could properly attest that these came from IBM's computer system or that the data stored in the system were not and/or could not have been tampered with before the same were printed out.** It is noteworthy that the computer unit and system in which the contents of the print-outs were stored were in the exclusive possession and control of petitioners since after private respondent was served his termination letter, he had no more access to his computer.[8]

As can be deduced from the IBM case, the basic requirements in labor cases regarding the admissibility of computer print-outs (of e-mails and similar documents) are the following:

1. To guarantee that the message sent was the same message received, the e-mail must be signed, either by the sender or the receiver; and
2. The computer printouts must be certified or authenticated by any company official who could properly attest that these came from the Company's computer system or that the data stored in the system were not or could not have been tampered with before the same were printed out.

Strictly speaking, the IBM case does not squarely address the problem of admissibility of electronic documents or data messages where there are no printouts or hardcopies to speak of.

---

[6] IBM Philippines, Inc., 305 SCRA at 600 and 601, citing Uichico v. NLRC 273 SCRA 35 (1997).

[7] Ibid., p. 601.

[8] Ibid., pp. 603-604.

With the E-Commerce Act in place, the question that may be posed in this regard is: "Are the requirements mentioned in the IBM case relative to the authentication of the computer print-outs enough to satisfy the provisions of the Act?" In other words, can we still say that the pronouncements of the Supreme Court in the IBM case are not affected, one way or the other, by the enactment of the Act?

Since the IBM case is a labor case, where identification, authentication and certification of documents can be done through an affidavit, without the latter being considered as hearsay even if the adverse party is not given the opportunity to actually cross-examine the affiant, then, arguably, the doctrinal pronouncements of the Supreme Court still apply even with the passage of the E-Commerce Act.

Electronic documents, electronic data messages or their printouts, when precented in evidence, must be properly identified and authenticated. Proof must also be shown that the messages sent were the same messages received. In the meantime that the Supreme Court has yet to decide a case on the basis of the E-Commerce Act, it is best to follow the requirements provided in the IBM case regarding admissibility of electronic documents or data messages. The IBM case recognizes the fact that even in labor cases, evidence must have a modicum of admissibility to be given some probative value. Otherwise, any doubt shall be resolved in favor of labor.

## Legal issues related to monitoring employees

Although most, if not all, of the provisions of the Act deal with the recognition and use of electronic commercial and non-commercial data messages, documents or contracts, the ultimate objective is to revolutionize, with the use of digital technologies, the way we handle information and do business. There are legal issues related to monitoring information on employees, the gathering of evidence, and access to computers assigned to employees. These issues require well-crafted policies on the use of digital technology in the workplace.

It is the declared policy of the State to, among others, "develop with appropriate training programs and institutional policy changes, human resources for the information age, a labor force skilled in the use of information and communications technology and a population capable of operating and utilizing electronic appliances and computers."[9]

[9] Sec. 2 of the Act.

The modern workplace uses digital information technology in the form of desktop computers, database servers, facsimile machines, electronic mail, electronic networks, interconnected informations systems, and the Internet to routinely process, store and transmit data for many important transactions.

A company's technology infrastructure is a resource that may produce enormous business benefits. However, it may also be abused. It is therefore a practical necessity to monitor employees' and use of digital technologies, especially the Internet, on the following grounds:

1. The facilities may be used for non-business purposes, such as surfing the Web for personal purposes. [10]

2. Employers may be liable for inappropriate e-mail or Internet related activities of their employees. In most cases, employee e-mail or Usenet postings carry the employer's name or trade mark as part of the employee's e-mail address. Defamatory statements sent outside the company by employees may, therefore, be attributed to the employer.[11]

Under Philippine laws, employers are liable for acts committed by their employees in the course of their employment. Article 2180 of the New Civil Code in part provides, thus:

> The owners and managers of an establishment or enterprise are likewise responsible for damages caused by their employees in the service of the branches in which the latter are employed or on the occasion of their functions.

Also, under our Penal Code, employers engaged in any kind of industry are liable for felonies committed by their employees in the discharge of their duties.[12]

3. Employers have an obligation to provide a work environment free of discrimination and harassment. Inappropriate material circulated internally can create a problem. One concern is the potential liability for sexually explicit messages sent to other employees. Such e-mail messages can be used to support a harassment or discrimination case.[13]

Pornographic images downloaded by employees are another big problem. If pornographic images are downloaded and displayed on an employee's monitor, then that can also contribute to a finding that the employer had allowed the creation of a hostile work environment for other employees.[14]

---

[10] See Alan Gahtan, "Monitoring Employee Communications", January 1997.

[11] Ibid.

[12] Article 103 of the Revised Penal Code.

[13] Ibid.

[14] Ibid.

Section 5 of R.A. 7877 Anti-Sexual Harassment Act of 1995 provides that the employer or head of office is liable *in solidum* for damages arising from the acts of sexual harassment committed in the employment, education or training environment if the employer or head office is informed of such acts by the offended party and no immediate action is taken on the complaint.

4. Much of the content accessible on the Internet is protectable by copyright, or intellectual property rights in general and needs to be used appropriately. The ease with which such content may be reproduced and an employee's belief that his actions are for the benefit of his employers may lead him to infringe on such content.[15]

Employers, however, must take care not to infringe on an employee's privacy rights or violate laws prohibiting the interception of private communications. Suppose it becomes necessary for an employer to monitor his employees' use of e-mail and access messages stored in their computers, can the employer legally do so?

Article III, Section 3(1) of our Constitution provides that "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." In implementation of this provision, the Anti-Wire Tapping Act (R.A. 4200) prohibits "any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept or record" the same, or to communicate the contents thereof to any other person.

The provisions of RA 4200 might have become outmoded. It can be said that the equipment mentioned in the law—dictaphones and dictographs—cannot be extended to computers or other equipment used for hacking or cracking per se. If one's system has been destroyed, that may be considered as malicious mischief; if something has been stolen from it, that would be theft. However, the mere act of unauthorized access may not be punishable.[16] The applicability of the constitutional provision earlier cited to e-mail communications is likewise doubtful considering that we have yet to see a Philippine case directly dealing with the matter.

---

[15] Ibid.

[16] E.C. Lallana, R.S. Quimbo, and Z.B. Andam, "E-Primer: An Introduction to E-Commerce," January 2000, p. 9.

The relevant provisions of the E-Commerce Act may be found in Sections 31, 32 and 33 (a), thus:

> SEC. 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 use of the plaintext, electronic signature or file and solely for the authorized purposes. x x x.
>
> SEC. 32. Obligation of Confidentiality. - Except for the purposes authorized under this Act, any person who obtained access to electronic key, electronic data message or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.
>
> SEC. 33 (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 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.

The unauthorized access or interference with a computer or information and communication system is punishable. The applicability of the cited provisions to personal computers is clear. This is not necessarily the case, however, with respect to information and communication systems in the workplace. In this case, it seems that the privacy of an employee is somewhat restricted.

Many of the case decided in this regard were in the United States and in most cases they tended to side with the employer. In one American case,[17] a federal district court held that an employee who was fired for the contents of an e-mail he sent on a company computer had no grounds to complain of wrongful termination. The court held that there was no privacy right, even though the employer had repeatedly promised not to intercept e-mail on its system. In that case, the employer had advised its employees that all e-mail communications would remain confidential

[17] Smith vs. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa., 1996).

and that e-mail communications could not be used against its employees as grounds for termination. An employee who was fired for sending what the Company deemed to be inappropriate and unprofessional comments to his supervisor using the e-mail system sued the company. The court dismissed the employee's claim stating that it did not find a reasonable expectation of privacy in the communication notwithstanding the assurance by management.

A case in California, brought by an e-mail administrator who was fired by Epson for complaining that her e-mail had been read was likewise dismissed, notwithstanding that Epson had told its employees that their e-mail was confidential.[18]

A similar lawsuit filed against Nissan Motor Company alleging tortious interception of employee e-mail messages was also unsuccessful. In the Nissan case, the California Court of Appeals affirmed a trial court's decision that the employees did not have a reasonable expectation of privacy because they had signed a waiver form which provided that it was "company policy that employees ... restrict their use of company-owned computer hardware and software to company business."[19]

In *U.S. v. Simons*,[20] Simons, an engineer at the Foreign Bureau of Information Services at the CIA, was convicted of receiving and possessing child pornography that he received via the Internet at his government office and computer. The policy of the employer was that the use of the Internet at the office was only for government business and that the employer could audit the computer at any time. Simons appealed, contending that the search and seizure of the pornography files was a violation of the Fourth Amendment. However, the court held that there was no improper search and seizure; the employer had the right to enter the employee's office and computer without a warrant since the search was for the purpose of obtaining evidence of work-related misconduct. Whether the misconduct was criminal or not does not matter. Simons had no expectation of privacy in files downloaded from the Internet in light of the employer's policy.

Based on the cases cited, it seems that an employer can reasonably restrict the right to privacy of communication of an employee. The restriction must of course have a reasonable connection with the performance of the employee of his duties and responsibilities. This

---

[18] See Alan Gahtan, "Monitoring Employee Communications", January 1997.

[19] Ibid.

[20] F.3d - (2000 WL 223332, 4th Cir.)

prerogative of the employer is based on the fact that the business itself and all equipment being used in furtherance of the business are the properties of the employer.

All told, the provisions of the Act on lawful access and hacking or cracking must be read within the context of the interplay between the rights and privileges of employers and employees in the workplace.

## Well-crafted policies on digital technology in the workplace

Computers and the Internet are increasingly becoming part of the workplace. This could create problems for companies which do not have a well-crafted policies on employees' use of the Internet, e-mail and computer systems in general.

According to **Mark Pomeroy,**[21] in his article **"Internet and Computer Use Policies,"** a well-crafted policy must contain the following:

*1. Purpose clause.* The policy should include a statement of the purpose of giving employees access to computer systems and the Internet. Internet "surfing" or any other computer activity unrelated to work duties must be prohibited. The policy should not to suggest that an employee has access "rights" to computer systems or the Internet. Access should be described as an additional "tool" owned by the employer and provided strictly for the employee's performance of job duties.

*2. Ownership.* The policy should make it clear that electronic documents and e-mail messages are the property of the company and should be for business use only. If employers allow a certain amount of personal use of computer resources and e-mail, the policy should so state. Employees must be reminded, however, that even personal documents and e-mails are not private and may be monitored by the management.

*3. Term provision.* While the length of time during which an employee may actually enjoy Internet or computer access may be the entire duration of employment, the policy should allow employer flexibility to revise the policy toward allowing the employer to withdraw Internet, e-mail or computer access. Such change in policy or withdrawal of access may reflect changes in the law and workplace changes such as a change in the employee's job duties, changes in technology, changes in the company's system, changes in the policy based on the company's

---

[21] Mark Pomeroy is a partner in the corporate department of Bricker & Eckler LLP and chairs the cyberlaw practice area. He can be contacted at mpomeroy@bricker.com.

experience with Internet or computer access, the company's determination that access does not contribute to business profitability or employee performance.

*4. Proscribed uses.* Include in the policies a reasonably understandable description of proscribed uses and identify categories of uses permitted and not permitted. Such proscribed uses may include offensive, unlawful and harassing communications of any kind. Computer use may also be limited to work-related functions and not extended to personal activities such as party invitations or personal correspondences. The employees should be notified, through the policies, as to whether personal e-mail is an accepted or proscribed use. In addition, the policies should use language that encompasses all functions that are proscribed. For instance, do not simply proscribe employee access to sites that contain sexually explicit materials, but expressly proscribe visiting such site; downloading material from such site; interacting with such site, including making purchases from the site; and leaving such site on the employee's screen for others to see.

*5. Company publicity.* The policies should include clear guidelines on the limits to which company information may be given out through chat groups, e-mail, and other public forums. "Cybersmear", in which a company finds itself the subject of Internet rumors and disparaging remarks, can be started by employees and can frequently spiral out of control of the company. There should be a clear prohibition on the release of any company information through electronic or other means unless such publicity is part of an employee's job.

*6. Remote use.* If employees are permitted to access the company's Internet or computer system from their homes or other locations outside the company's premises, the policy should spell out the terms of such access, including how much, if any, use may be made of this company's resource by family members or others outside of the organization.

*7. Software.* The policy should address whether or not employees may download software from the Internet and install such software on their assigned workstations.

*8. Privacy.* The policy should provide notice to employees that they should not expect their Internet activity, including visiting web sites and communicating by e-mail, to be private communications. If the company currently monitors or intends to monitor employee use of the Internet, including incoming and outgoing personal and business e-mail, these may at any time be monitored, copied, and used for all legitimate lawful purposes of the employer. The policy should also advise employees

regarding the lingering effects of an e-mail, that is, that it may not be "gone" just because one hits the "delete" button and that the employer may still have access to it.

*9. Passwords.* The policy should be clear about employee use and sharing of passwords with management or other employees.

*10. Wide distribution e-mails.* The policy should include information on when, if ever, an employee can send a company-wide e-mail, what topics are permissible, and what prior approvals, if any, are required.

*11. News groups and list serves.* The policy should clearly advise employees as to whether or not they are authorized to visit or subscribe to news groups or list serves.

*12. Noncompliance.* The policy should include the consequences of noncompliance and the right of the employer to decide when the policy has been breached.

## Conclusion

It remains to be seen how electronic contracting will actually affect labor relations. Evidentiary issues and problems will surely arise.

While we have noted that several cases in the United States were decided in favor of the employers, it should not be safely assumed that employers have an unlimited right to monitor employees' use of the digital technologies in the workplace or unlimited authority to act on whatever is discovered. Employers' rights must always be exercised in relation to the rights of employees.