



Republic of the Philippines
Supreme Court
Manila

A.M. No. 08-1-16-SC

**RULE ON THE WRIT
OF *HABEAS DATA***

EFFECTIVE FEBRUARY 2, 2008

MANILA, PHILIPPINES
JANUARY 2008



Republic of the Philippines
Supreme Court
Manila

EN BANC

A.M. No. 08-1-16-SC

RULE ON THE WRIT OF *HABEAS DATA*

RESOLUTION

Acting on the recommendation of the Chairperson and Members of the Committee on Revision of the Rules of Court submitting for this Court's consideration and approval the proposed Rule on the Writ of *Habeas Data*, the Court Resolved to APPROVE the same.

This Resolution shall take effect on February 2, 2008, following its publication in three (3) newspapers of general circulation.

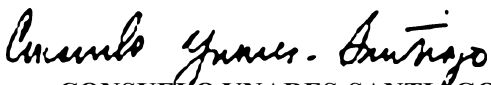
January 22, 2008.

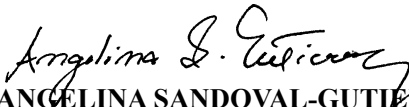
A handwritten signature in black ink, appearing to read "R. S. Puno", written over a printed name.

REYNATO S. PUNO

Chief Justice


LEONARDO A. QUISUMBING
Associate Justice


CONSUELO YNARES-SANTIAGO
Associate Justice


ANGELINA SANDOVAL-GUTIERREZ
Associate Justice

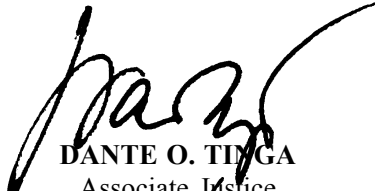

ANTONIO T. CARPIO
Associate Justice


MA. ALICIA AUSTRIA-MARTINEZ
Associate Justice



RENATO C. CORONA
Associate Justice

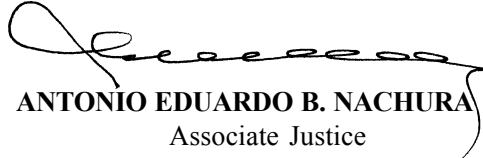

CONCHITA CARPIO MORALES
Associate Justice

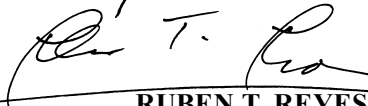

ADOLFO S. AZCUNA
Associate Justice


DANTE O. TINGA
Associate Justice

(on official leave)
MINITA V. CHICO-NAZARIO
Associate Justice


PRESBITERO J. VELASCO, JR.
Associate Justice


ANTONIO EDUARDO B. NACHURA
Associate Justice


RUBEN T. REYES
Associate Justice


TERESITA J. LEONARDO-DE CASTRO
Associate Justice

RULE ON THE WRIT OF *HABEAS DATA*

SECTION 1. *Habeas Data*.—The writ of *habeas data* is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.

SEC. 2. *Who May File*.—Any aggrieved party may file a petition for the writ of *habeas data*. However, in cases of extralegal killings and enforced disappearances, the petition may be filed by:

- (a) Any member of the immediate family of the aggrieved party, namely: the spouse, children and parents; or
- (b) Any ascendant, descendant or collateral relative of the aggrieved party within the fourth civil degree of consanguinity or affinity, in default of those mentioned in the preceding paragraph.

SEC. 3. *Where to File*.—The petition may be filed with the Regional Trial Court where the petitioner or respondent resides, or that which has jurisdiction over the place where the data or information is gathered, collected or stored, at the option of the petitioner.

The petition may also be filed with the Supreme Court or the Court of Appeals or the Sandiganbayan when the action concerns public data files of government offices.

SEC. 4. *Where Returnable; Enforceable*.—When the writ is issued by a Regional Trial Court or any judge thereof, it shall be returnable before such court or judge.

When issued by the Court of Appeals or the Sandiganbayan or any of its justices, it may be returnable before such court or any

justice thereof, or to any Regional Trial Court of the place where the petitioner or respondent resides, or that which has jurisdiction over the place where the data or information is gathered, collected or stored.

When issued by the Supreme Court or any of its justices, it may be returnable before such Court or any justice thereof, or before the Court of Appeals or the Sandiganbayan or any of its justices, or to any Regional Trial Court of the place where the petitioner or respondent resides, or that which has jurisdiction over the place where the data or information is gathered, collected or stored.

The writ of *habeas data* shall be enforceable anywhere in the Philippines.

SEC. 5. *Docket Fees.*—No docket and other lawful fees shall be required from an indigent petitioner. The petition of the indigent shall be docketed and acted upon immediately, without prejudice to subsequent submission of proof of indigency not later than fifteen (15) days from the filing of the petition.

SEC. 6. *Petition.*—A verified written petition for a writ of *habeas data* should contain:

- (a) The personal circumstances of the petitioner and the respondent;
- (b) The manner the right to privacy is violated or threatened and how it affects the right to life, liberty or security of the aggrieved party;
- (c) The actions and recourses taken by the petitioner to secure the data or information;
- (d) The location of the files, registers or databases, the government office, and the person in charge, in possession or in control of the data or information, if known;
- (e) The reliefs prayed for, which may include the updating, rectification, suppression or destruction of the database or information or files kept by the respondent.

In case of threats, the relief may include a prayer for an order enjoining the act complained of; and

- (f) Such other relevant reliefs as are just and equitable.

SEC. 7. *Issuance of the Writ.*—Upon the filing of the petition, the court, justice or judge shall immediately order the issuance of the writ if on its face it ought to issue. The clerk of court shall issue the writ under the seal of the court and cause it to be served within three (3) days from its issuance; or, in case of urgent necessity, the justice or judge may issue the writ under his or her own hand, and may deputize any officer or person to serve it.

The writ shall also set the date and time for summary hearing of the petition which shall not be later than ten (10) work days from the date of its issuance.

SEC. 8. *Penalty for Refusing to Issue or Serve the Writ.*—A clerk of court who refuses to issue the writ after its allowance, or a deputized person who refuses to serve the same, shall be punished by the court, justice or judge for contempt without prejudice to other disciplinary actions.

SEC. 9. *How the Writ Is Served.*—The writ shall be served upon the respondent by the officer or person deputized by the court, justice or judge who shall retain a copy on which to make a return of service. In case the writ cannot be served personally on the respondent, the rules on substituted service shall apply.

SEC. 10. *Return; Contents.*—The respondent shall file a verified written return together with supporting affidavits within five (5) work days from service of the writ, which period may be reasonably extended by the Court for justifiable reasons. The return shall, among other things, contain the following:

- (a) The lawful defenses such as national security, state secrets, privileged communication, confidentiality of the source of information of media and others;
- (b) In case of respondent in charge, in possession or in control of the data or information subject of the petition:

- (i) a disclosure of the data or information about the petitioner, the nature of such data or information, and the purpose for its collection;
 - (ii) the steps or actions taken by the respondent to ensure the security and confidentiality of the data or information; and
 - (iii) the currency and accuracy of the data or information held; and
- (c) Other allegations relevant to the resolution of the proceeding.

A general denial of the allegations in the petition shall not be allowed.

SEC. 11. *Contempt.*—The court, justice or judge may punish with imprisonment or fine a respondent who commits contempt by making a false return, or refusing to make a return; or any person who otherwise disobeys or resists a lawful process or order of the court.

SEC. 12. *When Defenses May Be Heard in Chambers.*—A hearing in chambers may be conducted where the respondent invokes the defense that the release of the data or information in question shall compromise national security or state secrets, or when the data or information cannot be divulged to the public due to its nature or privileged character.

SEC. 13. *Prohibited Pleadings and Motions.*—The following pleadings and motions are prohibited:

- (a) Motion to dismiss;
- (b) Motion for extension of time to file opposition, affidavit, position paper and other pleadings;
- (c) Dilatory motion for postponement;
- (d) Motion for a bill of particulars;
- (e) Counterclaim or cross-claim;
- (f) Third-party complaint;
- (g) Reply;

- (h) Motion to declare respondent in default;
- (i) Intervention;
- (j) Memorandum;
- (k) Motion for reconsideration of interlocutory orders or interim relief orders; and
- (l) Petition for *certiorari*, *mandamus* or prohibition against any interlocutory order.

SEC. 14. *Return; Filing.*—In case the respondent fails to file a return, the court, justice or judge shall proceed to hear the petition *ex parte*, granting the petitioner such relief as the petition may warrant unless the court in its discretion requires the petitioner to submit evidence.

SEC. 15. *Summary Hearing.*—The hearing on the petition shall be summary. However, the court, justice or judge may call for a preliminary conference to simplify the issues and determine the possibility of obtaining stipulations and admissions from the parties.

SEC. 16. *Judgment.*—The court shall render judgment within ten (10) days from the time the petition is submitted for decision. If the allegations in the petition are proven by substantial evidence, the court shall enjoin the act complained of, or order the deletion, destruction, or rectification of the erroneous data or information and grant other relevant reliefs as may be just and equitable; otherwise, the privilege of the writ shall be denied.

Upon its finality, the judgment shall be enforced by the sheriff or any lawful officer as may be designated by the court, justice or judge within five (5) work days.

SEC. 17. *Return of Service.*—The officer who executed the final judgment shall, within three (3) days from its enforcement, make a verified return to the court. The return shall contain a full statement of the proceedings under the writ and a complete inventory of the database or information, or documents and articles inspected, updated, rectified, or deleted, with copies served on the petitioner and the respondent.

The officer shall state in the return how the judgment was enforced and complied with by the respondent, as well as all

objections of the parties regarding the manner and regularity of the service of the writ.

SEC. 18. *Hearing on Officer's Return.*—The court shall set the return for hearing with due notice to the parties and act accordingly.

SEC. 19. *Appeal.*—Any party may appeal from the judgment or final order to the Supreme Court under Rule 45. The appeal may raise questions of fact or law or both.

The period of appeal shall be five (5) work days from the date of notice of the judgment or final order.

The appeal shall be given the same priority as *habeas corpus* and *amparo* cases.

SEC. 20. *Institution of Separate Actions.*—The filing of a petition for the writ of *habeas data* shall not preclude the filing of separate criminal, civil or administrative actions.

SEC. 21. *Consolidation.*—When a criminal action is filed subsequent to the filing of a petition for the writ, the latter shall be consolidated with the criminal action.

When a criminal action and a separate civil action are filed subsequent to a petition for a writ of *habeas data*, the petition shall be consolidated with the criminal action.

After consolidation, the procedure under this Rule shall continue to govern the disposition of the reliefs in the petition.

SEC. 22. *Effect of Filing of a Criminal Action.*—When a criminal action has been commenced, no separate petition for the writ shall be filed. The reliefs under the writ shall be available to an aggrieved party by motion in the criminal case.

The procedure under this Rule shall govern the disposition of the reliefs available under the writ of *habeas data*.

SEC. 23. *Substantive Rights.*—This Rule shall not diminish, increase or modify substantive rights.

SEC. 24. *Suppletory Application of the Rules of Court.*—The Rules of Court shall apply suppletorily insofar as it is not inconsistent with this Rule.

SEC. 25. *Effectivity.*—This Rule shall take effect on February 2, 2008 following its publication in three (3) newspapers of general circulation.

RATIONALE FOR THE WRIT OF *HABEAS DATA*

“Over one’s mind and over one’s body the individual is sovereign.”

—John Stuart Mill, *On Liberty*

INTRODUCTION

In every society, an individual has the right to live with other beings, (as social animals, in the crude words of Plato) and yet remain sovereign in one’s own dominion, one’s private domain. This is the foundation of the right to privacy—the right of the individual to insist upon his or her individuality and to control information, the dissemination of which would render the individual’s sovereignty inutile.

In the words of a famous American jurist, the right to privacy is the inalienable right of an individual “to be let alone.”¹ In legal history, the privacy of an individual takes its roots from common law, which recognized a man’s house as his castle, impregnable even to the monarchy and its officers engaged in the execution of its commands.

The publication in 1890 of the *Harvard Law Review* article “The Right to Privacy” by Samuel Warren and Louis Brandeis (later Justice Brandeis) forever changed legal literature and subsequent jurisprudence when they popularized the right to privacy as an independent legal right. With extreme foresight ahead of their time, Warren and Brandeis declared in 1890:

...[That] the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.

¹ THOMAS M. COOLEY, COOLEY ON TORTS 29 (2d ed. 1888); cited in Warren & Brandeis, *The Right to Privacy*, 4 HARV. LAW REV. 193, 195 (1890).

Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then, the “right to life” served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle.

...The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone.”²

Warren and Brandeis opened the portals to a more systematic study of the distinctive principles upon which the right to privacy is based. Recent developments, however, have shown that the said right covers broader aspects of human activity – the individual’s family, home and reputation. Indeed, no less than “The Universal Declaration of Human Rights,” in Article 12, states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Countries, such as France, protect privacy explicitly in their constitutions.³ The U.S. Constitution does not explicitly express the

² Warren & Brandeis, *supra* note 1, at 194, 195-196.

³ See THE FRENCH DECLARATION OF THE RIGHTS OF MAN AND OF THE CITIZEN.

right to privacy, yet the U.S. Supreme Court has repeatedly recognized, albeit implicitly, such a right in its efforts to preserve one's control over one's personal image. The Supreme Court of the United States, however, has found that the U.S. Constitution contains "penumbras" that implicitly grant a right to privacy against government intrusion. In *Griswold v. Connecticut* (1965),⁴ for example, the U.S. Supreme Court recognized that privacy was within the legal penumbra of the Bill of Rights, particularly in the First, Third, Fourth, Fifth and Ninth Amendments.

In *Griswold*, the Supreme Court explained that even though a right to privacy was not specifically articulated in the Constitution, "[the] right to privacy [is] older than the Bill of Rights—older than our political parties." The Court then established that the right to privacy was a fundamental right.

As Professor Coquia noted:

The right to privacy has been expressed several thousands of years ago with the maxim that "a man's house is his castle." The expectation of privacy within one's home is found in the *Talmud*, the Jewish civil and religious law and the Code of Hammurabi. These principles eventually have been incorporated in the Bills of Rights in several state constitutions. The Philippines in its Malolos Constitution adopted in 1899 states that "no person shall enter the domicile of a Filipino or foreigner residing in the Philippine Islands without his consent, except in urgent cases of fire, flood, earthquake, or other natural danger or unlawful aggression proceeding from within, or in order to assist a person calling for help." The Americans in their fight for independence from England questioned the quartering of armed troops in their homes.⁵

Other countries without constitutional privacy protections have laws protecting privacy, such as the United Kingdom's Data

⁴ *Griswold v. Connecticut*, 381 U.S. 479, 14 L. Ed. 2d 510 (1965).

⁵ Jorge Coquia, *The National Computerized Identification Reference System as Violation of the Right to Privacy: A Review of the Principles and Jurisprudence on Privacy as Human Right*, 293 SCRA 201, 202 (1998).

Protection Act of 1998 or Australia's Privacy Act of 1988. The European Union requires all member states to legislate to ensure that citizens have a right to privacy, through directives such as Directive 95/46.

I. THE RIGHT TO INFORMATIONAL PRIVACY

Generally, the right to privacy now involves the most basic rights of individual conduct and choice. The right to privacy includes the right of the person to prevent intrusion upon certain thoughts and activities, including freedom of speech and freedom to form or join associations. The right to privacy also includes the constitutional freedoms from unreasonable searches and seizures and from self-incrimination.⁶

Since the years following World War II, a powerful undercurrent of thought has evolved with respect to privacy, focused on personal information. The second half of the 20th century saw technological advances that made it increasingly possible to monitor and track persons as a result of the amazing amounts of personal identifying data that could be stored in ever more efficient ways. Governments that had always wanted to keep tabs on their citizens now had the means to do so and, with the paranoia that attended the Cold War, acquired a harrowing sense of urgency.

As innovations in computer technology continued at an incredible pace, authors and commentators began to warn of a future in which governments could use personal data to track and control the masses. To many, the right to be let alone was taking on a meaning different from the one that Warren and Brandeis had in mind. The new understanding of "information privacy" held that information was power, and that the increasing availability of personal data created a real danger that this power would be abused.

In *Whalen v. Roe*,⁷ a New York statute required the recording, in a centralized computer file, of the names and addresses of persons who obtained, pursuant to a doctor's prescription, certain drugs for

⁶ *Id.* at 203.

⁷ *Whalen v. Roe*, 429 U.S. 589 (1977).

which there were both lawful and unlawful markets. The statute prohibited public disclosure of the patient's identity. The U.S. Supreme Court held that the statute did not violate the patient and doctor relationship, but solidified the right to information privacy.⁸

The use of computers to accumulate, store, process, retrieve and transmit data has greatly advanced research methods. The new technology, however, poses new threats to privacy⁹ because it interferes with and may deprive individuals of the right to control the flow of information about themselves.

Information privacy is a prominent concept used in American constitutional law and designed to safeguard the ability of a person to restrict dissemination of personal information. Alan Westin, in a seminal book on the right to privacy, focused on the levels of information in the lives of each one of us. He analogized it to a series of circles within circles. The innermost circle contains the things about ourselves that we tell no one. The next innermost circle contains the things about us that are known only by those with whom we are most intimate. The circles continue until one reaches the information that is known by all.¹⁰

Computer technology has advanced rapidly with the global Internet system.¹¹

The computer system and other media tend to intrude upon privacy, as they can handle personal information by disseminating evidence of present and past actions or associations, even without the individual's consent. There is also the probability of introducing inaccurate information over which the individual has no control.¹²

From the time of our birth, through time we attended school to the period of our employment, pieces of information about ourselves—including our social associations—are recorded. We may have filled up numerous forms with information about ourselves,

⁸ *Id.* at 214.

⁹ Coquia, *supra* note 5 at 214.

¹⁰ See ALAN F. WESTIN, *PRIVACY AND FREEDOM* 33 (1964).

¹¹ Coquia, *supra* note 5, at 215.

¹² *Id.*

without any idea that the information we have given would one day be put together and made available to others at different times and for various purposes. Information of a privileged character can be fed into a computer machine, which certainly is an invasion of one's privacy.¹³

II. PHILIPPINE JURISPRUDENCE ON THE RIGHT TO PRIVACY

The right to privacy has recently emerged from frozen amber. The piecemeal and scattered provisions of privacy protection clauses in the 1987 Constitution and the growing amount of privacy jurisprudence has given life to the right to privacy.

In *Arnault v. Nazareno* (87 Phil. 29 [1950]), the petitioner invoked, before an investigation of the Blue Ribbon Committee of the Philippine Senate, the right to privacy in his dealings with other persons. The Supreme Court held in that case that there was no violation of the right to privacy. Since then, there has been a shift to a modern jurisprudential theory, which respects and upholds the right to privacy.

In *Morfe v. Mutuc* (92 SCRA 424), the Supreme Court had the occasion to rule on the existence of the right to privacy, despite dismissing the action for declaratory judgment challenging the validity of the provisions of the Anti-Graft and Corrupt Practices Act (Republic Act No. 3019). In *Morfe*, the questioned law required all public officers to submit in January of each year a statement of their assets and liabilities. The petitioner alleged that the statute was an unlawful invasion of the constitutional right to privacy, implicit in the prohibition on unreasonable searches and seizures and of the right against self-incrimination. The Supreme Court did not find merit in the contention that the statement was invalid, because the law did not call for the disclosure of information, an act that would infringe on the right to privacy of any person. Such pronouncement bore heavily in subsequent jurisprudence a most potent call for the delineation of what would infringe a person's right to privacy. *Morfe* recognized the constitutional right to privacy as laid down in *Griswold v. Connecticut*.¹⁴

¹³ *Id.*

¹⁴ See *Griswold*, *supra* note 4.

In *Ramirez v. Court of Appeals*,¹⁵ the Supreme Court strongly recognized the right to privacy of a person. The Court clarified therein that even a person privy to a communication who recorded a private conversation with another without the knowledge of the latter would qualify as a violator under Section 1 of R.A. No. 4200.

In *Ople v. Torres*,¹⁶ the Supreme Court declared:

...[T]he right to privacy does not bar all incursions into individual privacy. The right is not intended to stifle scientific and technological advancements that enhance public service and the common good. It merely requires that the law be narrowly focused and a compelling interest justifies such intrusions. Intrusions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions. We reiterate that any law or order that invades individual privacy will be subjected by this Court to strict scrutiny.¹⁷

The basic attribute of an effective right to informational privacy is the right of individuals to control the flow of information concerning or describing them. It is, however, a right that must be balanced by legitimate public concerns. To deprive individuals of their power to control or determine with whom to share information of their personal details would deny them of their right to their own personhood. For the essence of the constitutional right to informational privacy goes to the very heart of a person's individuality, an exclusive and personal sphere upon which the state has no right to intrude without any legitimate public concern.

As the erosion of personal privacy by computer technology and advanced information systems accelerates, the individual's ability to control their use diminishes.

There is more than a chilling prospect that one's profile formed from the gathering of data from various sources may divulge one's

¹⁵ *Ramirez v. Court of Appeals*, G.R. No. 93833, September 28, 1995, 248 SCRA 590.

¹⁶ *Ople v. Torres*, 354 Phil. 948 (1998).

¹⁷ *Id.* at 985.

private information to the public. There is also the unsettling thought that these data may be inaccurate, outdated or, worse, misused. There is, therefore, a pressing need to provide for judicial remedies that would allow the summary hearing of the unlawful use of data or information and to remedy possible violations of the right to privacy.

III. THE WRIT OF *HABEAS DATA*

In several Latin American countries, *habeas data* has attained the status not only of a procedural legal mechanism, but of a direct constitutional right.¹⁸ The scope and concept of *habeas data* vary from country to country. In general, it is designed to protect, by means of an individual complaint presented to a constitutional court, the image, privacy, honor, information, self-determination and freedom of information of a person.

The first Latin American country to implement *habeas data* was the Federal Republic of Brazil. In 1988, the Brazilian legislature voted for a new Constitution, which included a novel right never seen before: the *habeas data* individual complaint. It is expressed as a full constitutional right under Article 5, Title II of the 1988 Brazilian Constitution, which provides thus:

Habeas Data shall be granted: (1) to ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character; (2) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative.¹⁹

This constitutional provision was further bolstered by Brazil's National Congress in a 1997 regulatory law (*Congreso Nacional de Brasil, Lei 9507*).

¹⁸ Andreas Guadamuz, *Habeas Data: An Update on Latin America Data Protection Constitutional Right*, paper presented during the 16th BILETA Annual Conference, Edinburgh, Scotland, April 9-10, 2001.

¹⁹ 1988 Constitution of the Federal Republic of Brazil, Art. 5, §71. Available online at: <http://www.georgetown.edu/LatAmerPolitical/Constitutions/Brazil/btitle2.html> (last accessed November 15, 2007).

Following the Brazilian example, Colombia incorporated the *habeas data* right in its 1991 Constitution. The 1991 Colombian Constitution, as reformulated by the 1997 version, recognizes the right to individual privacy and recognizes that the citizens shall have “the right to know, access, update and rectify any information gathered about them in databases, both public and private.”²⁰ After that, many countries followed suit and adopted the new legal tool in their respective constitutions: Paraguay in 1992, Peru in 1993, Argentina in 1994, and Ecuador in 1996.

The 1992 Paraguay Constitution followed the example set by Brazil, but provided a stronger protection. Article 135 of the Paraguayan Constitution provides:

Everyone may have access to information and data available on himself or assets in official or private registries of a public nature. He is also entitled to know how the information is being used and for what purpose. He may request a competent judge to order the updating, rectification, or destruction of these entries if they are wrong or if they are illegitimately affecting his rights.²¹

Aside from giving the individual the right to find out what information is being kept about him or her, the Paraguay Constitution also recognizes the right to find out for what use and purpose such data were collected. The petitioner is also given the opportunity to question the data and argue for their “updating, rectification, or destruction.”²²

The Peruvian Constitution likewise recognizes *habeas data*. In Article 200, Section 3 of the Constitution of Peru, there is a similar provision much like that in Brazil’s and Paraguay’s. Moreover, the Peruvian legislature was quick enough to provide for

²⁰ 1997 Colombian Constitution, Art. 15 (*Constitucion Politica de Colombia*), available online at <http://www.georgetown.edu/LatAmerPolitical/Constitutions/Colombia/Colombia.html> (last accessed November 15, 2007).

²¹ 1992 Paraguay Constitution, art. 135, translated by Peter Heller, available online at http://www.uni-wuezburg.de/law/pa00t__.html (last accessed November 15, 2007).

²² *Id.*

a regulatory law that would take effect on April 18, 1995. The regulatory law recognized not only the procedural guarantee of updating one's data as contained in manual or physical records, but also one's right to update one's "automated" data or those personal data kept and supplied by any "information service, automated or not."²³ In this model, the *habeas data* remedy may be enforced against automated or digitized records.

In Argentina, the writ of *habeas data* is not specifically called *habeas data*, but is subsumed into the Argentine writ of *amparo*. Article 43 of the Argentine Constitution, under the title "*Amparo*" or protection, states:

Any person may file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired.²⁴

The Argentine version, despite not being called *habeas data*, is more comprehensive than other Latin American models. The Argentine model includes the judicial remedy to enforce one's right to access, rectify, update, or destroy the data, like in the Paraguay model. The Argentine version also guarantees the confidentiality of personal or private information and specifically provides for the protection of journalistic privilege, presumably of the lofty democratic role that the press enjoys.

Legal literature has recounted the varying effects of *habeas data*. Legislatures in Latin America are constantly restudying the regulatory and substantive roles and limitations of the writ. Our legislature can also study the applicability of *habeas data* to data

²³ 1993 Peruvian Political Constitution (*Constitucion Politica del Peru*), Art. 2, §6.

²⁴ Constitution of the Argentine Nation of 1853, as amended by the 1994 Constitutional Reform, Article 43 (as translated by the Argentine Congress).

protection especially in this day and age of information technology, when privacy can easily be pierced by the push of a button.

Be that as it may, several studies have shown remarkable uses of the *habeas data* writ – uses that were not really intended by its developers. An “unforeseen effect” of this judicial remedy is that it has become “an excellent Human Rights tool mostly in the countries that are recovering from military dictatorships.”²⁵ Thus, in Paraguay, an action for *habeas data* was successfully filed to assert the right to view the records from a police station, bringing to light several atrocities that had been committed at that site. In a landmark case in Argentina, its Supreme Court held that the *habeas data* rule applied implicitly to the families of the deceased in a case involving extralegal killing and enforced disappearance. This was a recognition of the right of the families of the disappeared, usually victims of the military regime, to request access to police and military records otherwise closed to them—and, in essence, establishing a right to truth.

The **right to truth** has been a fundamental principle central to the task of confronting transitions to democracy and the legacy of massive human rights violations in Latin America. This right entitles the families of disappeared persons to know the totality of circumstances surrounding the fates of their relatives and imposes an obligation of investigation on the part of governments. This right is particularly crucial in cases of political disappearances, which frequently imply secret executions of detainees without any trial, followed by the concealment of the bodies for the purpose of erasing all material traces of the crime and securing impunity for the perpetrators.

The right to truth is a component of the right to life, liberty and security. The right to truth is the bedrock of the rule of law, which the State is obligated to protect with all obstinacy under national and international law.²⁶ No family member can sleep well without knowing the true whereabouts of his or her father, mother, brother, sister, son or daughter. Indeed, truth has and will always set us free.

²⁵ Guadamuz, *Habeas Data*, n. 43.

²⁶ See Art. 8, Universal Declaration of Human Rights (UDHR).

For all these reasons and more, the writ of *habeas data* will provide our people with an additional remedy that would hopefully terminate the extralegal killings and enforced disappearances plaguing our country. The writ of *habeas data* will not only complement the writ of *amparo*. It will stand as an independent remedy to enforce the right to informational privacy. For all persons have the right to access information about themselves, especially if it is in the possession of the government. Any violation of this right ought to give the aggrieved person the remedy to go to court to modify, remove, or correct such misinformation. The right to access and control personal information is essential to protect one's privacy, honor and personal identity, even as it underscores accountability in information gathering.

In the history of law, filing an individual complaint before courts to invoke constitutional rights has long been granted a substantive recognition. The first and perhaps most famous of these complaints is called *habeas corpus*, roughly translated as "You should have the body." The writ of *habeas corpus* is a guarantee against deprivation of a person's liberty. It originated in the Middle Ages in England, recognized in the several versions of the *Magna Carta*, so that a person held in custody was brought before a judge or court to determine whether the detention was lawful or otherwise. Throughout history, several writs have been developed to protect the rights of the individual against the State. In the United States of America, for instance, the writ of *mandamus* has become popular to command a governmental agency to perform a ministerial function, so that a person may enjoy the benefits of a common government; in Latin American countries, particularly Mexico and Argentina, there is a writ of *amparo*, which is a general guarantee covering a whole gamut of constitutional rights; in Taiwan, the *respondeat superior* writ makes a superior liable for the acts of the subordinate; and so on and so forth.

Recently, the Supreme Court *en banc* has promulgated the Rule on the Writ of *Amparo*. The Philippine version of the writ of *amparo* has been designed to protect the most basic right of a human being—one's right to life, liberty and security as guaranteed not only by the **Philippine Constitution of 1987**, but also by the **1898 Declaration of Philippine Independence** and the **Universal**

Declaration of Human Rights of 1948.

The *habeas corpus* writ has been used for more than five centuries now. The writ of *amparo* has been recognized for more than five decades. Compared with these two, the writ of *habeas data* has a very short history.²⁷ The writ of *habeas corpus* can be traced way back to as early as 1215 in the United Kingdom; it was subsequently codified in 1679.²⁸ The writ of *amparo* can be traced back to the last fifty decades of democratization in Latin American countries. The direct predecessor of the writ of *habeas data* is the Council of Europe's 108th Convention on Data Protection of 1981. The writ of *habeas data* may be said to be the youngest legal mechanism studied by comparative law. The writ is young, because it appeals to the present generation. A comparative law scholar has described *habeas data* as "a procedure designed to safeguard individual freedom from abuse in the information age."²⁹

The European Data Protection Convention of 1981 was convened to develop safeguards to secure the privacy of the individual by way of regulating the processing of personal information or data. *Habeas data* was initially developed in the early 1980s Europe, where countries like Germany founded its use upon the constitutional recognition of the right to individual self-determination. In Latin American countries, the writ has found use against perennial problems regarding the protection of the individual against human rights abuses.

In recent years, recourse to the action of *habeas data* has become a fundamental instrument for investigation into human rights violations committed during past military dictatorships in the Western Hemisphere. Family members of disappeared persons have used actions for *habeas data* to obtain information concerning government conduct, to learn the fate of disappeared persons, and to exact accountability. Thus, these actions constitute important means to guarantee the right to privacy and, as a complementary right, the "right to truth."

²⁷ See Andres Guadamuz, *Habeas Data and the European Data Protection Directive*, in THE JOURNAL OF INFORMATION, LAW AND TECHNOLOGY (JILT) (2001).

²⁸ The *Habeas Corpus* Act of 1679. See 1 BLACKSTONE, COMMENTARIES 131 (1st ed. 1765-1769).

²⁹ ENRIQUE FALCON, HABEAS DATA: CONCEPTO Y PROCEDIMIENTO 23 (1996) (translation provided).

By designing a Philippine version of the *habeas data*, we can further our resolve to finally bring to a close the problem of extralegal killings and enforced disappearances in our country, a spectral remain of the Martial Law regime.

The Supreme Court is not blind to the happenings of the present. Ever always is there a need to balance the powers of the government with the right of the individual, so that we can all enjoy that ever elusive “just and humane society” where, over one’s own mind and body, one remains sovereign.

ANNOTATION TO THE WRIT OF *HABEAS DATA*

The writ of *habeas data* is an independent remedy to protect the right to privacy, especially the right to informational privacy. The privacy of one's person, family and home is a sanctified right in the history of constitutional law.¹ It has been said that a man's home is his kingdom—which even the king has to respect.²

In *Morfe v. Mutuc*,³ the Supreme Court ruled thus:

The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection. The language of Prof. Emerson is particularly apt: “The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen.” This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state. In contrast, a system of limited government safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector—protection, in other words, of the dignity and integrity of the individual—has become increasingly important as modern society has developed. All the forces of technological age—industrialization, urbanization, and organization—operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity

¹ Irene Cortes, *The Constitutional Foundations of Privacy*, in EMERGING TRENDS IN LAW (University of the Philippines Press: 1983).

² *Id.*

³ *Morfe v. Mutuc*, 130 Phil. 415 (1968), 22 SCRA 424 (per C.J. Fernando).

to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society.⁴

The writ of *habeas data* is also a remedy to protect the right to life, liberty or security of a person from violation or threatened violation by an unlawful act or omission of a public official or employee or of a private individual or entity. It complements the remedies of the writ of *amparo* and writ of *habeas corpus*.

The highlights of the proposed Rule, section by section, are as follows:

SECTION 1. *Habeas Data*.—The writ of *habeas data* is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.

Coverage. The section defines the parameters of the writ of *habeas data*. It complements the writ of *amparo* to protect victims whose right to life, liberty or security has been violated or threatened with violation by public authorities or by private persons or entities. Through the writ of *habeas data*, the victim or the members of his or her family, can compel the respondents to reveal such data or information necessary to enforce their right to life, liberty or security.

The writ of *habeas data*, however, can be availed of as an independent remedy to enforce one's right to privacy, more specifically the right to informational privacy. The remedies against the violation of such right can include the updating, rectification, suppression or destruction of the database or information or files in possession or in control of respondents.

SEC. 2. *Who May File*.— Any aggrieved party may file a petition for the writ of *habeas data*. However, in cases of extralegal killings and enforced disappearances, the petition may be filed by:

⁴ *Id.* at pp. 444-445.

- (a) **Any member of the immediate family of the aggrieved party, namely: the spouse, children and parents; or**
- (b) **Any ascendant, descendant or collateral relative of the aggrieved party within the fourth civil degree of consanguinity or affinity, in default of those mentioned in the preceding paragraph.**

Who May File. The right to privacy is a personal right; hence, it is the aggrieved party who can seek the remedy of the writ of *habeas data* for its enforcement. Where, however, the petitioner is a minor or an incapacitated person or one who is not of sound mind, or, in any case where a legal guardian is required, then such legal guardian may file the petition for and on behalf of the ward in accordance with the Rules of Court, which applies suppletorily for the purposes of this Rule.

In cases involving extralegal killings and disappearances, however, the writ may be filed by members of the family of the aggrieved party following an order of priority. The same rule applies to the writ of *amparo*.

SEC. 3. Where to File.—**The petition may be filed with the Regional Trial Court where the petitioner or respondent resides, or that which has jurisdiction over the place where the data or information is gathered, collected or stored, at the option of the petitioner.**

The petition may also be filed with the Supreme Court or the Court of Appeals or the Sandiganbayan when the action concerns public data files of government offices.

Courts Where Petition May Be Filed. Regional Trial Courts (RTCs) are the primary venues for the filing of a writ of *habeas data*. These courts are spread all over the country. The petition usually involves determination of facts which trial courts can better resolve. However, the Supreme Court, the Court of Appeals, or the Sandiganbayan may also entertain the petition especially where it involves public data files of government offices.

SEC. 4. *Where Returnable; Enforceable.*—When the writ is issued by a Regional Trial Court or any judge thereof, it shall be returnable before such court or judge.

When issued by the Court of Appeals or the Sandiganbayan or any of its justices, it may be returnable before such court or any justice thereof, or to any Regional Trial Court of the place where the petitioner or respondent resides, or that which has jurisdiction over the place where the data or information is gathered, collected or stored.

When issued by the Supreme Court or any of its justices, it may be returnable before such Court or any justice thereof, or before the Court of Appeals or the Sandiganbayan or any of its justices, or to any Regional Trial Court of the place where the petitioner or respondent resides, or that which has jurisdiction over the place where the data or information is gathered, collected or stored.

The writ of *habeas data* shall be enforceable anywhere in the Philippines.

Return of Writ. This section is a modified version of the corresponding provision on the rule of the writ of *amparo* because the *habeas data* writ may be made returnable to the RTC that has jurisdiction over the place where the data or information is gathered, collected or stored as *forum actus* – the forum of the place where the act in question was done.

SEC. 5. *Docket Fees.*— No docket and other lawful fees shall be required from an indigent petitioner. The petition of the indigent shall be docketed and acted upon immediately, without prejudice to subsequent submission of proof of indigency not later than fifteen (15) days from the filing of the petition.

Partial Exemption. Indigents are exempted from payment of docket fees in accord with the Court's policy of widening the poor's access to justice. However, considering that the petition will entail costs in logistics and documentary production, docket fees shall be paid by those with the capacity to pay.

SEC. 6. *Petition.*—A verified written petition for a writ of *habeas data* should contain:

- (a) The personal circumstances of the petitioner and the respondent;
- (b) The manner the right to privacy is violated or threatened and how it affects the right to life, liberty or security of the aggrieved party;
- (c) The actions and recourses taken by the petitioner to secure the data or information;
- (d) The location of the files, registers or databases, the government office, and the person in charge, in possession or in control of the data or information, if known;
- (e) The reliefs prayed for, which may include the updating, rectification, suppression or destruction of the database or information or files kept by the respondent.

In case of threats, the relief may include a prayer for an order enjoining the act complained of; and

- (f) Such other relevant reliefs as are just and equitable.

Content. The provision requires specific and verified allegations in support of the petitioner's cause of action. It also requires the petitioner to allege the courses of action he or she has undertaken to protect the right to privacy or the right to life, liberty or security of the petitioner. All requirements are intended to prevent the misuse of the writ for "fishing expedition" purposes.

SEC. 7. *Issuance of the Writ.*—Upon the filing of the petition, the court, justice or judge shall immediately order the issuance of the writ if on its face it ought to issue. The clerk of court shall issue the writ under the seal of the court and cause it to be served within three (3) days from its issuance; or, in case of

urgent necessity, the justice or judge may issue the writ under his or her own hand, and may deputize any officer or person to serve it.

The writ shall also set the date and time for summary hearing of the petition which shall not be later than ten (10) work days from the date of its issuance.

Issuance. The writ is issued as a matter of course when on the face of the petition it ought to issue. The writ will require respondent to file a return, which is the comment or answer to the petition.

The provision requires that the writ should set the date of summary hearing on the petition, which shall not be later than ten (10) work days from the date of the issuance of the writ.

SEC. 8. *Penalty for Refusing to Issue or Serve the Writ.*—A clerk of court who refuses to issue the writ after its allowance, or a deputized person who refuses to serve the same, shall be punished by the court, justice or judge for contempt without prejudice to other disciplinary actions.

Penalties. The provision is a modified version of a similar provision in Rule 102, governing petitions for a writ of *habeas corpus*.

SEC. 9. *How the Writ Is Served.*—The writ shall be served upon the respondent by the officer or person deputized by the court, justice or judge who shall retain a copy on which to make a return of service. In case the writ cannot be served personally on the respondent, the rules on substituted service shall apply.

Manner of Service. The writ should be served against the respondent in person. If personal service cannot be made, the rules on substituted service shall apply. This will avoid the situation in which a public respondent in the military/police service would be conveniently assigned to a “secret mission” to frustrate personal service.

SEC. 10. *Return; Contents.*—The respondent shall file a verified written return together with supporting affidavits within five (5) work days from service of the writ, which period may be reasonably extended by the Court for justifiable reasons. The return shall, among other things, contain the following:

- (a) The lawful defenses such as national security, state secrets, privileged communication, confidentiality of the source of information of media and others;
- (b) In case of respondent in charge, in possession or in control of the data or information subject of the petition:
 - (i) a disclosure of the data or information about the petitioner, the nature of such data or information, and the purpose for its collection;
 - (ii) the steps or actions taken by the respondent to ensure the security and confidentiality of the data or information; and
 - (iii) the currency and accuracy of the data or information held; and
- (c) Other allegations relevant to the resolution of the proceeding.

A general denial of the allegations in the petition shall not be allowed.

Contents of the Return. The respondent shall submit a verified written return to answer the allegations of the petition. General denials will not suffice. The respondent may interpose his or her lawful defense which may include nondisclosure of data or information that involves national security, a state secret, privileged information or other defenses sanctioned by law, the Rules of Court and decisions of the Supreme Court.

Where the respondent is in charge, in possession or in control of the data or information, the respondent is required to disclose the

steps or actions he or she has taken to ensure the security, confidentiality and accuracy of the information. Again, this requirement is intended to strengthen the right to privacy.

SEC. 11. *Contempt.*—The court, justice or judge may punish with imprisonment or fine a respondent who commits contempt by making a false return, or refusing to make a return; or any person who otherwise disobeys or resists a lawful process or order of the court.

Contempt. The power to cite for contempt is an inherent power of a court to compel obedience to its orders and to preserve the integrity of the judiciary. A finding of contempt of court may result from making a false return which is tantamount to not making a return; a refusal to make a return; disobedience to a lawful order; and resistance to a lawful process. A fine or an imprisonment may be imposed on a person found guilty of contempt of court in accordance with the Rules of Court.

SEC. 12. *When Defenses May Be Heard in Chambers.*—A hearing in chambers may be conducted where the respondent invokes the defense that the release of the data or information in question shall compromise national security or state secrets, or when the data or information cannot be divulged to the public due to its nature or privileged character.

Defenses. There are defenses that cannot be heard in open court in view of their confidential nature. They should be heard and examined by the Court in chambers with proper precautions to safeguard their secrecy. Respondents, however, are duty-bound to disclose them to the Court.

SEC. 13. *Prohibited Pleadings and Motions.*—The following pleadings and motions are prohibited:

- (a) Motion to dismiss;
- (b) Motion for extension of time to file opposition, affidavit, position paper and other pleadings;

- (c) Dilatory motion for postponement;
- (d) Motion for a bill of particulars;
- (e) Counterclaim or cross-claim;
- (f) Third-party complaint;
- (g) Reply;
- (h) Motion to declare respondent in default;
- (i) Intervention;
- (j) Memorandum;
- (k) Motion for reconsideration of interlocutory orders or interim relief orders; and
- (l) Petition for *certiorari*, *mandamus* or prohibition against any interlocutory order.

Prohibited Pleadings. The enumerated pleadings and motions are prohibited to expedite the proceedings. Since the right to life, liberty or security of a person is at stake, the proceedings should not be delayed. The right to privacy is similarly important.

Certiorari Jurisdiction of the Supreme Court. If the court, justice or judge gravely abuses his or her discretion in issuing orders, as when they will compromise national security, the aggrieved party is not precluded from filing a petition for *certiorari* with the Supreme Court, which, under the Constitution, may not be deprived of its *certiorari* jurisdiction.

SEC. 14. *Return; Filing.*—In case the respondent fails to file a return, the court, justice or judge shall proceed to hear the petition *ex parte*, granting the petitioner such relief as the petition may warrant unless the court in its discretion requires the petitioner to submit evidence.

Ex Parte Hearing. Upon failure to file a return, the Court should proceed to hear the petition *ex parte*. It may require the petitioner to present further evidence in support of his or her allegations and, upon that basis, render judgment.

SEC. 15. *Summary Hearing.*—The hearing on the petition shall be summary. However, the court, justice or judge may call for a preliminary conference to simplify the issues and determine the possibility of obtaining stipulations and admissions from the parties.

Summary Nature. The *habeas data* hearing is summary in nature and is held from day to day until completed. The right to life, liberty or security and the right to privacy need immediate vindication. Be that as it may, the court, justice or judge, using reasonable discretion, is not precluded from holding a preliminary conference, if such conference will aid in the speedy disposition of the petition.

SEC. 16. *Judgment.*—The court shall render judgment within ten (10) days from the time the petition is submitted for decision. If the allegations in the petition are proven by substantial evidence, the court shall enjoin the act complained of, or order the deletion, destruction, or rectification of the erroneous data or information and grant other relevant reliefs as may be just and equitable; otherwise, the privilege of the writ shall be denied.

Upon its finality, the judgment shall be enforced by the sheriff or any lawful officer as may be designated by the court, justice or judge within five (5) work days.

Speedy Judgment. The court, justice or judge is obliged to render judgment within ten (10) days after submission of the petition for decision. The short period is demanded by the extraordinary nature of the writ.

Standard of Judgment. Where the allegations of the petition are proven by substantial evidence, the privilege of the writ shall be granted. In case of threats, the court shall enjoin the act complained of. In case the data or information have already been gathered, collected or stored, the court shall order their deletion, destruction, or rectification as prayed for in the petition. It may issue other relevant reliefs as may be just and equitable.

The court shall deny the privilege of the writ and dismiss the petition in case the allegations of the petition are not proven by substantial evidence.

SEC. 17. *Return of Service.*—The officer who executed the final judgment shall, within three (3) days from its enforcement, make a verified return to the court. The return shall contain a full statement of the proceedings under the writ and a complete inventory of the database or information, or documents and articles inspected, updated, rectified, or deleted, with copies served on the petitioner and the respondent.

The officer shall state in the return how the judgment was enforced and complied with by the respondent as well as all objections of the parties regarding the manner and regularity of the service of the writ.

Officer's Return. This is a modified version of A.M. No. 02-1-06-SC, the Rule on Search and Seizure in Civil Actions for Infringement of Intellectual Property Rights, promulgated January 22, 2002. Section 17 thereof provides in full:

SEC. 17. Sheriff's return.—The sheriff who executed the writ shall, within three (3) days from its enforcement, make a verified return to the court that issued the writ. The return shall contain a full statement of the proceedings under the writ and a complete inventory of the documents and articles searched, inspected, copied, or seized and impounded, with copies served on the applicant, the defendant or expected adverse party, and the Commissioner.

If not all of the documents and articles enumerated in the order and writ were seized, the sheriff shall so report to the court and state the reasons therefor. All objections of the defendant, expected adverse party or person in charge of the premises, as to the manner and regularity of the service of the writ shall be included by the sheriff in his return.

The detailed return is to compel the officer to take extra care in enforcing the judgment of the Court.

SEC. 18. *Hearing on Officer's Return.*—The court shall set the return for hearing with due notice to the parties and act accordingly.

Report on Enforcement and Compliance. There is a need for a hearing to determine compliance of the parties and to inform the court of the sufficiency of the enforcement steps taken by the officer. In this hearing, the Court shall determine if there is any objection to the manner of execution of the judgment on the part of any party. This will assure the Court that its decision has been faithfully followed.

SEC. 19. *Appeal.*—Any party may appeal from the judgment or final order to the Supreme Court under Rule 45. The appeal may raise questions of fact or law or both.

The period of appeal shall be five (5) work days from the date of notice of the judgment or final order.

The appeal shall be given the same priority as *habeas corpus* and *amparo* cases.

Appeal. Appeal shall be taken under Rule 45, with the modification that the appellant may raise questions of fact or law or both.

SEC. 20. *Institution of Separate Actions.*—The filing of a petition for the writ of *habeas data* shall not preclude the filing of separate criminal, civil or administrative actions.

Prerogative Writ. Like the writ of *amparo*, the writ of *habeas data* partakes of the nature of a prerogative writ. It is not a criminal, civil, or administrative suit. Hence, it does not suspend the filing of criminal, civil or administrative actions.

SEC. 21. *Consolidation.*—When a criminal action is filed subsequent to the filing of a petition for the writ, the latter shall be consolidated with the criminal action.

When a criminal action and a separate civil action are filed subsequent to a petition for a writ of *habeas data*, the petition shall be consolidated with the criminal action.

After consolidation, the procedure under this Rule shall continue to govern the disposition of the reliefs in the petition.

Consolidation. In case a petition for the writ of *habeas data* is filed prior to the institution of a criminal action, or prior to a separate civil action, the petition shall be consolidated with the criminal action. This Rule shall govern the disposition of the reliefs for *habeas data* after consolidation.

SEC. 22. *Effect of Filing of a Criminal Action.*—When a criminal action has been commenced, no separate petition for the writ shall be filed. The reliefs under the writ shall be available to an aggrieved party by motion in the criminal case.

The procedure under this Rule shall govern the disposition of the reliefs available under the writ of *habeas data*.

Effect of Criminal Proceeding. This section contemplates a situation in which a criminal action has already been filed, and the commencement of the *habeas data* action is barred. This provision seeks to avoid the difficulties that may be encountered when the *habeas data* action is allowed to proceed separately from the criminal action. Two courts trying essentially the same subject may issue conflicting orders.

The *habeas data* reliefs, however, are made available to the aggrieved party through proper motions in the court where the criminal case is pending. The disposition of these motions shall be governed by this Rule.

SEC. 23. *Substantive Rights.*—This Rule shall not diminish, increase or modify substantive rights.

No Diminution, Increase or Modification of Substantive Rights. The rule-making power of the Supreme Court has been expanded in Article VIII, Section 5(5) of the 1987 Constitution. It provides that the Supreme Court shall have the power to

“[p]romulgate rules *concerning the protection and enforcement of constitutional rights* [which] shall not diminish, increase, or modify substantive rights...”⁵

The Supreme Court clarified what constitutes procedural rules in *Fabian v. Desierto*, viz:

[T]he test whether the rule really regulates procedure, that is, the *judicial process for enforcing rights and duties recognized by substantive law* and for justly administering remedy and redress for a disregard or infraction of them. If the rule takes away a vested right, it is not procedural. If the rule creates a right such as the right to appeal, it may be classified as substantive matter; but *if it operates as a means of implementing an existing right, then the rule deals merely with procedure.*⁶

SEC. 24. *Suppletory Application of the Rules of Court.*—The Rules of Court shall apply suppletorily insofar as it is not inconsistent with this Rule.

Suppletory Application of the Rules of Court. The Rules of Court shall supplement the Rule on *habeas data* as far as it is applicable. This new Rule shall prevail and shall not be affected by prior inconsistent rules, resolutions, regulations or circulars of the Supreme Court.

SEC. 25. *Effectivity.*—This Rule shall take effect on February 2, 2008,⁷ following its publication in three (3) newspapers of general circulation.

Date of Effectivity. The section marks the date of effectivity of the Rule and its publication requirement. The Committee deemed it proper that the birth of the Rule on the Writ of *Habeas Data* in the Philippines should coincide with our celebration of Constitution Day.⁸

⁵ 1987 PHIL. CONST. Art. VIII, §5, ¶ 5 (emphasis supplied).

⁶ G.R. No. 129742, September 16, 1998, at 22-23 citing 32 AM. JUR. 2d, Federal Practice and Procedure, §505, at 936; *People v. Smith*, 205 P. 2d 444.

⁷ To coincide with Constitution Day.

⁸ Proclamation No. 211 (1998) declares February 2 of every year as Constitution Day to celebrate the ratification by the Filipino People of the 1987 Constitution.