

8 RMLNLUJ (2016) 31

Fight Against Terror & Financial Privacy: Striking the Right Balance

by
Kumar Askand Pandey*

I. INTRODUCTION

Right to privacy is an individual's right to be let alone in the absence of some reasonable public interest in a person's activities¹. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating the right.

The right to privacy is not mentioned in the Constitution, but the Supreme Court has interpreted Article 21 of the Constitution of India² as creating this right³. Though there is little statutory material protecting privacy rights of an individual in India, recent amendments in the Information Technology Act, 2000 (IT Act)⁴ underline the importance of this right.

In the United States, like India, the Constitution does not specifically mention the right to privacy as a constitutional right but the federal Supreme Court has interpreted several of the amendments as creating this right. One of such amendments is the Fourth Amendment, which stops the police and other government agents from searching individuals or their property without probable cause. Other amendments protect a person's freedom to make certain decisions about their bodies and their private lives without interference from the government. The due process clause of the



Page: 32

14th amendment generally only protects privacy of family, marriage, motherhood, procreation, and child rearing⁵.

In essence, privacy cannot be separated from a person's individuality. Individuals choose what they reveal in the public sphere, and what they keep private. Privacy allows an individual to delimitate his or her private and public spheres, an idea that is grounded in the human condition as a balance between individuality and social interaction. The distinction between the private and public spheres and its respect are traditional features of civilization. For the same reason, people put curtains on their windows or wear clothes. Whether someone has something to hide is not the issue. Such practices are necessary lines of demarcation between one's individuality and participation in society. In practical terms, the confidentiality due in financial affairs is akin to the professional secrecy of medical doctors or lawyers. It is intended to protect the individual against third parties, including the government⁶."

Financial privacy is an offshoot of privacy in general and as the term itself suggests, it is basically concerned with privacy of an individual in financial transactions. Financial institutions, including banks, owe it to their customers that their financial privacy would be respected⁷. Legislative framework is in place in many developing and developed economies providing for protection of financial privacy. Certain European countries have taken the issues of financial privacy to a higher level and therefore, such countries are regarded as banking heavens⁸. The prime example would be Austria and Switzerland⁹. However, similar to other rights, the right to financial privacy is subject to numerous exceptions and limitations. One such exception would be when the financial institutions disclose the financial secrets in criminal proceedings

concerning serious crimes e.g. money laundering and terrorism.

Strict financial privacy laws have become a matter of concern for the international community as the ill gotten money is often pumped in financing terrorist activities in different parts of the globe¹⁰.



Page: 33

India has been a victim of cross-border and home-bred terrorism for long. Finances are crucial in terrorism; therefore, laws are required to strike a balance between the financial privacy of an individual or entity and the interest of the country as a whole. Records of financial transactions are highly useful in ascertaining physical transactions, and are often the only evidence of their occurrence. Moreover, the financial proceeds of crime usually find their way to those who commissioned the crime. Many financial transactions, because of bookkeeping entries, required records, or the instruments themselves, reveal the identities of the payer and the payee, leaving a ready audit trail. Criminals conceal this evidence from law enforcement authorities by "laundering" their funds through financial institutions, allowing criminals to fund other legal or illegal ventures¹¹.

The object of this paper is to evaluate the financial privacy laws in India, comparing it with its counterpart in certain jurisdictions like U.S.A., U.K. and Switzerland and I shall argue that the notion of financial privacy have drastically changed in the last two decades so much so that it virtually does not exist anymore.

II. LEGAL RECOGNITION OF FINANCIAL PRIVACY

Financial privacy rights have their origin in common law and the first major recognition of this right came in the famous *Tournier* case¹² in the context of banker-customer relationship. The plaintiff was a customer of the defendant bank. A cheque was drawn by another customer of the defendant in favour of the plaintiff, who instead of paying it in to his own account indorsed it to a third person who had an account at another bank. On the return of the cheque to the defendant their manager inquired of the last named bank who the person was to whom it had been paid, and was told it was a bookmaker. That information the defendant disclosed to third persons.

It was held¹³ that the disclosure constituted a breach of the defendant's duty to the plaintiff, for though the information was acquired not through the plaintiff's account but through that of the drawer of the cheque, it was acquired by the defendant during the currency of the plaintiff's account and in their character as bankers. Bankes LJ stated that confidentiality may be breached:"

- i) Where disclosure is made under compulsion of law;
- ii) Where there is a duty to the public to disclose



Page: 34

- iii) Where the interests of the bank requires disclosure
- iv) Where the disclosure is made by the express or implied consent of the customer".

The decision was affirmed by the Court of Appeal in *Lipkin Gorman v. Karpnale Ltd.*¹⁴

Tournier has been the basis of financial privacy laws in common law jurisdictions and its principles have been codified in financial privacy legislations.

III. FINANCIAL PRIVACY LAWS IN THE U.S.A.

There has been a great deal of debate in the US about privacy in respect of Bank records and inspection thereof by the State. In *United States v. Miller*¹⁵, the majority of the Supreme Court laid down that once a person passes on cheques etc. to a bank, which indeed is in a position of a third party, the right to privacy of the document is no longer protected¹⁶. In response to *Miller*, Congress came forward with the Right to Financial Privacy Act, 1978¹⁷, which provided several safeguards to secure privacy, - namely - requiring reasonable cause and also enabling the customer to challenge the summons or warrant in a Court of law before it could be executed. It has been recognized that financial institutions must keep information received about their clients in the course of business secret and confidential¹⁸. In the United States a variety of legal doctrines, grounded in contract, agency, and tort theory, recognize and protect the interest of individuals in financial privacy. Some of these rights are codified in legislations which protects individual financial privacy rights from interference by the state.

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" (GLB Act) was signed into law on November 12, 1999 and became effective on July 1, 2001. The law modified previous federal laws and "allows for the creation of a financial holding company. Such companies may include a commercial bank and subsidiaries that conduct financial activities or activities incidental to financial activities".




In other words, GLB enables banks to engage in a whole line of financial activities. Late in the legislative process, legislators were concerned at the prospect that the consolidation of the financial industry would lead to privacy invasions. As a result of this concern, Title V was added to the GLB Act. Title V of the GLB Act requires financial institutions to provide an initial "clear and conspicuous" notice of privacy policies and practices to all customers, an annual notice of privacy policies, and an opportunity for consumers to opt out of disclosing protected financial information to nonaffiliated third parties¹⁹."

Responses to the GLB Act privacy rule have been mixed. Many privacy law scholars were critical of exceptions and the choices offered in the law". For example Pandozzi concluded that "Title V (GLB Privacy Section) is riddled with loopholes and exceptions that severely weaken, if not paralyze, the consumers' power to opt out of information sharing between financial institutions and nonaffiliated third parties"²⁰. Paul M. Schwartz argues that the GLB's promise falls short because the opt-out requirement burdens the consumer. He wrote, "The opt-out rule fails to impose any penalty on the party with superior knowledge — the financial entity — should negotiations over further use and transfer of data fail to occur. ... the GLB Act places the burden of bargaining on the less-informed party, the individual consumer"²¹.

Mostly, financial privacy is breached or is not available in terrorism and heinous financial fraud investigations. U.S. laws against terrorist financing²² are comprehensive, and they criminalize: (1) providing, or concealing or disguising the

nature, location, source or ownership of "material support or resources", knowing that they may be used to carry out a terrorist act²³, (2) the provision or attempted provision of "material support" (as defined

 Page: 36

in Section 2339A) to a foreign terrorist organization²⁴, and (3) providing or collecting, directly or indirectly, "funds" knowing or intending that they be used to carry out any act listed in the various conventions, protocols and treaties covered by the Terrorist Financing Convention, or any act intended to cause death or serious bodily injury to a civilian, or any person not taking an active part in the hostilities of a situation of armed conflict to intimidate a populations, to compel a government or international organization to do or abstain from doing any act²⁵.


Thus, in the national interest, financial privacy would not be honoured if the same leads to channeling funds for criminal and anti-national activities.

IV. U.K. FINANCIAL PRIVACY LAWS

The primary rule in UK banking law is that all information relating to the state of a customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account is confidential, subject to the four *Tournier* exceptions and the *Tournier* rules (including the exceptions) have been enacted in different legislations.

The first exception in *Tournier* permits the bank to disclose confidential information under compulsion of law. This may be either at common law or statute.

The Banking Act, 1979, was the first formal legal framework to banking regulation within the UK. Part V of the Banking Act, 1987, sets out restrictions on the disclosure of information without consent. It does not extend to any information within the public domain. Exceptions are set out at Sections 83 and 84. These permit, *inter alia*, restricted information may be released to an auditor if that information would assist the FSA in discharging its functions. Section 7 of the Bankers Books and Evidence Act, 1879, permits any party to legal proceedings to apply to the court for an order granting him permission to inspect and take copies of any entries in a banker's book, for the purposes of such proceedings. This power is discretionary, and will only be exercised with great caution. An order is only usually made against the account of the party who is involved in the litigation or, if it is in the name of some other person, the account which is really the account of the party. It will only be made against non parties in very exceptional circumstances. Further, there is an implied undertaking on discovery only to use the documents for the purposes of the action in which discovery is given.

 Page: 37

Various provisions under tax laws permit the Commissioners to decide whether or not in their opinion tax has been unlawfully evaded²⁶.

Therefore, the ambit of this exception is wide. However, it is only the office holder, such as the Administrator or liquidator that may make an application to the court for an order under this provision.

The police are entitled to obtain access to special procedure material for the

purposes of criminal investigation. If an order is made relating to bank confidential information, the bank is under no obligation to resist the order, nor to inform the customer that an order is being sought²⁷.

Section 177 of the Financial Services Act, 1986 allows the Secretary of State to appoint inspectors to carry out investigations to establish whether or not an offence of insider dealing has been committed. The Inspectors may order any person whom they consider may be able to give information to produce any documents in his possession or control.

The court may summon any person known or suspected to be in possession of any property of the company or supposed to be indebted to the company; or any person whom the court thinks capable of giving information concerning the promotion, formation, dealings, affairs or property of the company. It can require production of any records in his possession or control relating to these issues. The provision is not limited to documents required to reconstitute the state of the company's knowledge²⁸."

By Section 2, of the Criminal Justice Act, 1987, in cases of serious or complex fraud, the Director of the Serious Fraud Office may require any person to produce specified documents that appear to the Director to relate to any matter relevant to the investigation.

In 1989, the Treasury and the Bank of England set up the first independent review²⁹ on banking services law and practice within the UK. Its report is known as the 'Jack Report'³⁰. It recommended that the government should not further extend the statutory exceptions to the duty of confidentiality, without taking full account of the consequences for the banker/customer relationship".

However, the rising fear of terrorist financing and illegal channeling of finances have led to serious encroachments in the so called right to financial



privacy in the U.K. In certain circumstances, banks are obliged to disclose financial information and a failure to do so.

The anti-money laundering provisions stipulate that "It is an offence for someone to enter into or become concerned in an arrangement which knows or suspects facilitate the acquisition, retention use or control of criminal property. Disclosure must be made to the National Criminal Intelligence Service (NCIS)"³¹. Further, it is an offence to fail to report a person's engagement in any kind of illegal money-laundering when the information is acquired in the course of business if the defendant has knowledge or suspicion or reasonable grounds for knowledge or suspicion³².


It has been rightly observed that since 1984, when the Police and Criminal Evidence Act was passed, there has been a vast transformation in the range of legislation that invades the privacy of banking records, not just in relation to drug trafficking but also in relation to white-collar and other 'hard-to-convict' crime and thus bringing about the death of financial privacy³³.

V. POSITION IN SWITZERLAND

In Switzerland, citizens have the right to protection of financial privacy. Banks are required to maintain confidentiality concerning the financial affairs of their clients. Bank employees who violate that duty are liable to prosecution. Banking secrecy arises from provisions in the Swiss Civil Code concerning personal privacy, data protection law and banking legislation. However, the client may relieve the bank of its confidentiality, and allow it to disclose information covered by banking secrecy.

However, Swiss banking secrecy is not absolute. Numerous provisions of civil law, debt collection and bankruptcy law, criminal law, administrative criminal law, and mutual assistance in criminal matters provide for exceptions to banking secrecy. If there is sufficient suspicion of an offence, banking secrecy can be lifted against the client's will on the order of a judicial authority or a supervisory authority".

The Swiss financial centre has numerous instruments at its disposal to defend against assets originating from criminal offences. By international standards, the Swiss rules are very strict. They require in particular that the contracting party be identified when accepting assets and the origin of

 Page: 39

the assets clarified. The legal framework is provided by the Anti-Money Laundering Act³⁴.


Almost all of the Swiss population is of the opinion that financial privacy must be guaranteed, with 91% stating that they want bank clients' financial data to be protected against third parties (2010: 89%). In other words, it is not just about showing positive sentiment towards the banking sector. This is also reflected in the fact that bank-client confidentiality continues to enjoy the firm support of the Swiss population. As was the case in 2010, 73% of survey respondents believed that bank-client confidentiality should be preserved. Abolishing it for domestic clients would therefore enjoy little support³⁵. This explains the enviable position Switzerland holds as a banking heaven. However, in March 2009, Switzerland agreed to adopt Article 26 of the OECD Model Convention on international administrative assistance in tax matters. This makes it possible to exchange information for tax purposes with other countries in individual cases and upon specific and justified request, in cases of both tax fraud and tax evasion³⁶."

VI. FINANCIAL PRIVACY IN INDIA

Arguably, *Tournier* seems to be applicable in India³⁷ but the use of technology in the field of banking appears to have thrown up fresh challenges to banks in effectively fulfilling their obligation to maintain secrecy of the accounts of their customers flowing from the relationship of banker and customer as recognized by the law and courts".

A reference may be made to the Personal Data Protection Bill, 2006³⁸ which was introduced in the *Rajya Sabha* to provide for protection of personal data and information of an individual collected for a particular purpose, though the Bill has not been passed at all".

The principal banking legislation regulating banking affairs in India, the Banking Regulations Act, 1949 does not, in any way, provide the details of the conduct of the bank business. It only contemplates the registration of a bank, incorporation of a bank and thereafter puts the bank under the control

 Page: 40

of the Reserve Bank of India (RBI)³⁹. Chapter III of the RBI Act deals with collection and furnishing of credit information⁴⁰.

The RBI has power to collect and call for credit information from any banking company and also to furnish such information to any banking company⁴¹. Giving a glimpse of financial privacy rights, disclosure of credit information has been

prohibited⁴². Exceptions to this prohibition are more elaborate⁴³. Interestingly, in India, breach of financial privacy is not actionable⁴⁴. In 1974, an amendment made to the RBI Act, repealed the penalties for violation of the provisions of Chapter III A⁴⁵.



Page: 41

Thus, we see that the RBI Act does not provide for a robust financial privacy regime through which the financial privacy of individuals or entities could be safeguarded to any extent.

RBI has issued certain guidelines for banks and through these widely published and circulated guidelines dated 21.11.2005, has constituted a working group on regulatory mechanisms and for fair trade practices.

These guidelines came into effect as of 30th November, 2005 and covers a wide area pertaining to the rights of the customers and right to privacy, confidentiality, practice of debt collections, redressal of grievances and monitoring systems to be implemented by the banks⁴⁶.

In yet another "Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by banks", the RBI has sought to ensure the financial privacy of customers of banks, where the banks have outsourced some of their activities⁴⁷.

However, the spurt in money laundering and terrorism in India led to enactment of legislations which have virtually declared death of the right to financial privacy. Two principal legislations in this regard are the Prevention of Money Laundering Act, 2002 (PMLA), and the Unlawful Activities Prevention Act, 1967 (UAPA).

A. The IT Act, 2000

Section 43A of IT Act, deals with the aspect of compensation for failure to protect data. The Central Government has not prescribed the term 'sensitive personal data,' nor has it prescribed a "standard and reasonable security practice". Until these prescriptions are made, data is afforded security and protection only as may be specified in an agreement between the parties or as may be specified in any law. However, Explanation (ii) to Section 43A of IT Act is worded in such a way that there is lack of clarity whether it would be possible for banks, (or any body corporate) to enter into agreement which stipulate standards lesser than those prescribed by Central Government and in the event of the contradiction (between the standards prescribed by the Central Government and those in the agreement) which would prevail. Whether a negligence or *mala fide* on the part of the customer would make the financial institution liable for no fault of it or whether by affording too much protection to banks, a customer is made to suffer are the two extremes of the situation. The need is for striking a balance between consumer protection and protection of the banks from liability due to no fault



Page: 42

of theirs. Apart from affording protection to personal data, the IT Act also prescribes civil and criminal liabilities (Section 43 and Section 66 of IT Act respectively) to any person who without the permission of the owner or any other person who is in charge of a computer, computer system etc., *inter alia*, downloads, copies or extracts any data or damages or causes to be damaged any computer data base etc. In this context Section 72 and 72A of the amended IT Act are also of relevance. Section 72 of the IT

Act prescribes the punishment if any person who, in pursuance of the powers conferred under the IT Act has secured access to any electronic record, information etc and without the consent of the person concerned discloses such information to any other person then he shall be punished with imprisonment up to two years or with fine up to one lakh or with both. Section 72A of the IT Act, on the other hand, provides the punishment for disclosure by any person, including an intermediary, in breach of lawful contract. The purview of Section 72A, IT Act, is wider than Section 72, IT Act, and extends to disclosure of personal information of a person (without consent) while providing services under a lawful contract and not merely disclosure of information obtained by virtue of 'powers granted under the IT Act'".

B. The PMLA

The PMLA and the rules framed under it require every banking company, financial institution and intermediary, to furnish to Financial Intelligence Unit-India (FIU-IND), information relating to—

- (A) All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- (B) All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- (BA) All transactions involving receipts by non-profit organisations of value more than rupees ten lakhs, or its equivalent in foreign currency;
- (C) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;
- (D) All suspicious transactions whether or not made in cash⁴⁸."

PMLA lays down obligations on banking companies, financial institutions and intermediaries to maintain a record of all transactions of




prescribed nature and value and to also furnish information of such transactions to the Director⁴⁹. Also, Rule 8 of the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 specifies the time limit for furnishing of information.

In discharge of its obligation under the PMLA, the RBI has issued a "Know Your Customer (KYC) norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism (CFT)/Obligations of Banks under Prevention of Money Laundering Act, (PMLA), 2002"⁵⁰.

The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently⁵¹. The RBI is mindful of financial privacy of the customers of financial institutions and lays down that "Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer

is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information

 Page: 44

from the customer should be sought separately with his/her consent and after opening the account"⁵²."


Special emphasis in these guidelines is on combating financial support to terrorism⁵³.

C. The UAPA

The UAPA, which was originally enacted to deal with criminal syndicates and organized crimes, was drastically amended to curb the menace of terrorism as well. The amendments were made pursuant to the Resolutions 1267 (1999), 1333 (2000), 1363 (2001), 1390 (2002), 1455 (2003), 1526 (2004), 1566 (2004), 1617 (2005), 1735 (2006) and 1822 (2008) of the Security Council of the United Nations requiring the member States to take action against certain terrorists and terrorist organisations, to freeze the assets and other economic resources, to prevent the entry into or the transit through their territory, and prevent the direct or indirect supply, sale or transfer of arms and ammunitions to the individuals or entities listed in the Schedule (to the UAPA)⁵⁴.

Under Section 7 of the UAPA, the Central Government has the power to prohibit use of any funds for the purposes of unlawful association (as defined in the UAPA)⁵⁵. To check the arbitrary use of the power under this section and also to ensure financial privacy of the person/entity whose funds have been subjected to the operation of this provision, the aggrieved person may, within fifteen days of the prohibitory order, challenge the same in the court of the District Judge within whose local limits the aggrieved person ordinarily resides or carries out his business etc⁵⁶.

It is an offence under the UAPA to deal in the funds in spite of the prohibitory orders made under Section 7, and punishable with imprisonment up to three years and also fine. The subject matter of the prohibitory order may also be realized by imposing an additional fine to the tune of the value of the funds in respect to which the contravention has take place⁵⁷.

 Page: 45

Chapter 3 of the UAPA, specifically dealing with terrorism, declares it an offence to raise funds in any manner, in India or abroad, for directly or indirectly financing terrorist activities. Even an attempt to do so is punishable irrespective of the fact whether in fact the funds were actually used for the terrorist acts or not⁵⁸.

Knowingly holding of any property derived from commission of terrorist act is punishable with life imprisonment and fine⁵⁹.

UAPA declares that (1) No person shall hold or be in possession of any proceeds of terrorism.

(2) Proceeds of terrorism, whether held by a terrorist or terrorist organisation or terrorist gang or by any other person and whether or not such terrorist or other person is prosecuted or convicted for any offence under Chapter IV or Chapter VI, shall be liable to be forfeited to the Central Government or the State Government, as the case

may be, in the manner provided under this Chapter (V)⁶⁰. Under Section 25 of the UAPA, the investigating officer or the designated authority has powers to seize properties, which such officer believes to be proceeds of terrorism. An appeal against this order may be made to obviate arbitrariness⁶¹.

Where any property is seized or attached on the ground that it constitutes proceeds of terrorism and the court confirms the order in this regard under sub-section (6) of section 25, it may order forfeiture of such property, whether or not the person from whose possession it is seized or attached, is prosecuted in a court for an offence under Chapter IV or VI (of the UAPA)⁶².

Sections 27 and 28 of the UAPA respectively, ensure that the orders made by a competent court for the forfeiture under Section 26, pass the test of natural justice and an avenue for appeal against such order is open to the aggrieved person. The UAPA also contains a novel provision to obviate financial injury to any third person by operation of Section 25, whereby such third persons may prefer claims or make objection against seizure or attachment of any property⁶³.

Section 32 of the UAPA provides that any property transferred in any mode after the operation of Sections 25 and 27 shall be null and void. Section 33 of the UAPA stipulates an additional filtering mechanism



providing that during the trial of a person for offences under the UAPA, his properties shall stand attached if not already attached in accordance with the provisions of Chapter V of UAPA. Raising funds for terrorist organizations has been declared a punishable offence under Section 40 of the UAPA, and carries imprisonment up to fourteen years or fine or both. Financial institutions are under an obligation to furnish information concerning commission of offences being investigated under the UAPA⁶⁴. Failure to furnish information as required in Section 43 F is punishable⁶⁵.

D. Disclosure under the General Laws

Apart from the special legislations, PMLA and UAPA, there are several provisions in other general legislations encroaching upon the financial privacy norms.

Section 93(1) of the Code of Criminal Procedure, 1973 (Cr PC) which deals with power of the Court to issue 'search warrants' (a) where the Court has 'reason to believe' that a person to whom a summons or order under Section 91 (Cr PC) or a requisition under Section 92(1) (Cr PC) has been, or might be, addressed, - will not or would not produce the document or thing as required by summons or requisition, or (b) where such document or thing is not known to the Court to be in the possession of any person, or (c) where the Court considers that the purposes of any inquiry, trial or other proceeding under the Cr PC, will be served by a general search or inspection, it may issue a search-warrant; and the person to whom such warrant is directed, may search or inspect in accordance therewith and the provisions contained in the Cr PC. Under Section 93(2) of Cr PC, the Court may, if it thinks fit, specify in the warrant, the place or part thereof to which only the search or inspection shall extend; and the person charged with the execution of such warrant shall then search or inspect only the place or part so specified. A warrant to search for a document, parcel or other thing in the custody of the postal or telegraph authority, has to be issued by the District Magistrate or Chief Judicial Magistrate. Section 165 of the Cr PC deals with the power of a police officer to search. Under Section 165(1) Cr PC, he must have reasonable grounds for believing that anything necessary for the purpose of an investigation into any offence, which he is authorized to investigate, may be found in

any place within the limits of the police station and that such thing cannot, in his opinion, be otherwise obtained without undue delay. He has to record the grounds of his belief in writing and specify, so far as possible, the thing for which search is made. Section 166, Cr PC, refers to the question as to when an officer-in-charge of a police station may require another to issue search warrant”.



Page: 47

In the Income-tax Act, 1961 (ITA), elaborate provisions are made in regard to search and seizure in Section 132; power to requisition books of account etc. in Section 132A; power to call for information as stated in Section 133. Section 133(6), ITA, deals with power of officers to require any Bank to furnish any information as specified there. There are safeguards. Section 132, ITA, uses the words “in consequence of information in his possession, has reason to believe”. Section 132(1A), ITA, uses the words “in consequence of information in his possession, has reason to suspect”. Section 132(13), ITA, says that the provisions of the Cr PC, relating to searches and seizure shall apply, so far as may be, to searches and seizures under Sections 132(1) and 132(1A), ITA. There are also Rules made under Section 132(14), ITA. Likewise Section 132A (1), ITA, uses the words “in consequence of information in his possession, has reason to believe”. Section 133, ITA, which deals with the power to call for information from Bank and others, uses the words “for the purpose of this Act” and Section 133(6), ITA, permits a requisition to be sent to a bank or its officer. There are other Central and State statutes dealing with procedure for ‘search and seizure’ for the purposes of the respective statutes.

VII. CONCLUSION

No right is absolute and so is the right to financial privacy. The growing fear of terrorism and flourishing corruption and money laundering has forced the countries to have a relook at their financial privacy regime. The *Tournier* rule itself laid exceptions and the recent developments in India and other countries are only in consonance with those exceptions. Even the data protection legislations in different countries have created exceptions for disclosure of data for the purposes of prevention, detection and prosecution of crimes. The proposed Personal Data Protection Bill, 2006 seeks to strike a balance between the individual right to financial privacy and the country's interest in preventing and punishing criminal activities.

Terrorism and many other crimes thrive on finances. In fight against terrorism and organized crime including large scale swindling of money, the first casualty would be the notion of financial privacy and rightly so. An analysis of the RBI Act and guidelines, the PMLA, the UAPA and other general legislations leave no doubt that though the confidentiality of financial information is to be respected, the interest of the nation would be paramount even if that results in breach of financial privacy. The banker-customer relationship is intact but the relationship and the consequent legal obligations on the part of the financial institutions can not be a cloak to further anti-national activities. Unwarranted breach of confidentiality and banking secrecy would still give rise to a cause of action for damages, but the present legal mechanism in the sphere of financial privacy certainly marks the demise of its classical notion.

— — —

* Associate Professor (Law), Dr. Ram Manohar Lohiya National Law University, Lucknow. Author can be reached at ka_pandey@rmlnlu.ac.in.

¹ See, Warren and Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).

² Article 21 reads, "No person shall be deprived of his life and personal liberty except according to procedure established by law".

³ See, *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295; *Gobind v. State of M.P.*, (1975) 2 SCC 148 : AIR 1975 SC 1378; *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632 : AIR 1995 SC 264; *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301 : AIR 1997 SC 568; *Hinsa Virodhak Sangh v. Mirzapur Moti Kuresh Jamat*, (2008) 5 SCC 33 : AIR 2008 SC 1892.

⁴ See, the Information Technology (Amendment) Act, 2008.

⁵ *Thornburgh v. American College of Obstetricians and Gynecologists*, 90 L Ed 2d 779 : 476 US 747 (1986).

⁶ Pierre Bessard, *Individual Rights and the Fight Against "Tax Evasion"*, (December, 2011) LI-Paper, Liberales Institut, Switzerland, at p. 18.

⁷ Respecting financial privacy would, in principle, also mean protection of client/customer data furnished to the financial institutions.

⁸ <http://internationalliving.com/2007/12/12-14-07-banking> (accessed on 05/10/2016).

⁹ *Supra*, note 6.

¹⁰ Jean B. Weld, *Current International Money Laundering Trends and Anti-Money Laundering Co-operation Measures*, available at http://www.unafei.or.jp/english/pdf/RS_No83/No83_08VE_Weld3.pdf (accessed on 06/10/2016).

¹¹ Commission on Organized Crime, *The Cash Connection: Organized Crime, Financial Institutions and Money Laundering* (1984).

¹² *Tournier v. National Provincial and Union Bank of England*, (1924) 1 KB 461.

¹³ Per Bankes and Atkin L.JJ.

¹⁴ (1989) 1 WLR 1340.

¹⁵ 48 L Ed 2d 71 : 425 US 435 (1976).

¹⁶ *Miller* received widespread criticism in U.A.S. for obvious reasons. See, Richard Alexander, *Privacy, Banking Records and Supreme Court: A Before and After Look at Miller*, 10 SW Univ. L. Rev. (1978) 13.

¹⁷ 12 U.S.C. 3401.

¹⁸ Charles Thelen Plombeck, *Confidentiality and Disclosure: The Money Laundering Control Act of 1986 and Banking Secrecy*, 22 Int'l L. 69 (1988) at p. 69.

¹⁹ Sheng, Steve and Cranor, Lorrie Faith, "An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies" (2006). *Institute for Software Research*. Paper 33, available at <http://repository.cmu.edu/isr/33> (accessed on 09/03/2014).

²⁰ Neal R. Pandozzi, *Be Ware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, Miami Law Review 163 (2001).

²¹ Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (2004).

²² The UN Convention Against Terrorist Financing (1999) (Terrorist Financing Convention) defines terrorist financing as "the providing or collecting of funds by any means, directly or indirectly,... with the intention that they should be used or in the knowledge that they are to be used,... (a) to carry out an act which constitutes the offense of terrorism; (b) to carry out any other act intended to cause death or serious bodily injury to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act,... is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act; or (3) by any terrorist or terrorist organization (for any purpose)".

²³ 18 U.S.C. § 2339A (enacted in 1994).

²⁴ 18 U.S.C. § 2339B (enacted in 1996).

²⁵ 18 U.S.C. § 2339C (enacted in 2002).

²⁶ Sections 1, 2 of the Taxes Management Act, 1970.

²⁷ Section 9, Police and Criminal Evidence Act, 1984.

²⁸ Section 236(1), Insolvency Act, 1986.

²⁹ Banker/Customer Relationship Review Committee on Banking Services Law (1987).

³⁰ Cm 622 (1989).

³¹ Section 328, Proceeds of Crime Act, 2002.

³² Section 330, *Id.*

³³ Michael Levi, *The Death of Bank Secrecy in the U.K.*, Br. J. Criminol (1991) 31 (2) 109.

³⁴ www.efd.admin.ch/themen/wirtschaft/02314/index.html (accessed on 09/10/2016).

³⁵ Result of the opinion poll is available at <http://www.swissbanking.org/en/medienmitteilung-20110325> (accessed on 09/10/2016).

³⁶ *Supra*, note 34.

³⁷ See, *Kattabomman Transport Corpn. Ltd. v. State Bank of Travancore*, 1992 SCC OnLine Ker 95 : AIR 1992 Ker 351; *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 638 : 2006 III LLJ 540 Del.

³⁸ Bill No. XCI of 2006, available at http://164.100.24.219/BillsTexts/RBillTexts/asintroduced/XCI_2006.pdf (accessed on 12/10/2016).

³⁹ The Reserve Bank of India Act, 1934.

⁴⁰ *Id.*, Section 45 A (c) "credit information" means any information relating to—

- (i) the amounts and the nature of loans or advances and other credit facilities granted by a banking company to any borrower or class of borrowers;
- (ii) the nature of security taken from any borrower or class of borrowers for credit facilities granted to him or to such class;
- (iii) the guarantee furnished by a banking company for any of its customers or any class of its customers;
- (iv) the means, antecedents, history of financial transactions and the credit worthiness of any borrower or class of borrowers;
- (v) any other information which the Bank may consider to be relevant for the more orderly regulation of credit or credit policy.

⁴¹ *Id.* Sections 45 B & 45 C.

⁴² *Id.* Section 45 E (1): Any credit information contained in any statement submitted by a banking company under section 45C or furnished by the Bank to any banking company under section 45D, shall be treated as confidential and shall not, except for the purposes of this Chapter, be published or otherwise disclosed.

⁴³ *Id.* Section 45 E (2): Nothing in this section shall apply to —

- (a) the disclosure by any banking company, with the previous permission of the Bank, of any information furnished to the Bank under section 45C:
- (b) the publication by the Bank, if it considers necessary in the public interest so to do, of any information collected by it under section 45C, in such consolidated form as it may think fit without disclosing the name of any banking company or its borrowers:
- (c) the disclosure or publication by the banking company or by the Bank of any credit information to any other banking company or in accordance with the practice and usage customary among bankers or as permitted or required under any other law:

Provided that any credit information received by a banking company under this clause shall not be published except in accordance with the practice and usage customary among bankers or as permitted or required under any other law.

- (d) the disclosures of any credit information under the Credit Information Companies (Regulation) Act, 2005.

(3) Notwithstanding anything contained in any law for the time being in force, no court, tribunal or other authority shall compel the Bank or any banking company to produce or to give inspection of any statement submitted by that banking company under section 45C or to disclose any credit information furnished by the Bank to that banking company under section 45D.

⁴⁴ *Id.* Section 45F: No person shall have any right, whether in contract or otherwise, to any compensation for any loss incurred by reason of the operation of any of the provisions of this Chapter.

⁴⁵ Repealed by Section 15 of the Reserve Bank of India (Amendment) Act, 1974 (51 of 1974).

⁴⁶ <http://rbidocs.rbi.org.in/rdocs/notification/PDFs/71238.pdf> (accessed on 10/10/2016).

⁴⁷ <http://www.rbi.org.in/commonman/English/scripts/Notification.aspx?Id=40> (accessed on 10/10/2016).

⁴⁸ <http://fiuindia.gov.in/furnishing-overview.htm> (accessed on 11/10/2016).

⁴⁹ Section 12. (1) Every banking company, financial institution and intermediary shall —

(a) maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month.

(b) furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;

(c) verify and maintain the records of the identity of all its clients, in such a manner as may be prescribed.

Provided that where the principal officer of a banking company or financial institution or intermediary, as the case may be, has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

(2)(a) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of ten years from the date of transactions between the clients and the banking company or financial institution or intermediary, as the case may be.

(b) The records referred to in clause (c) of sub-section (1) shall be maintained for a period of ten years from the date of cessation of transactions between the clients and the banking company or financial institution or intermediary, as the case may be.

⁵⁰ <http://rbidocs.rbi.org.in/rdocs/notification/PDFs/MCKYCC010709.pdf> (accessed on 11/10/2016).

⁵¹ *Id.* Guidelines 1.1.

⁵² *Id.* Guidelines 2.1.

⁵³ *Id.* Guidelines 2.11.

⁵⁴ *See*, the preamble to the UAPA.

⁵⁵ Section 2 (p) of the UAPA: "unlawful association" means any association,—

(i) which has for its object any unlawful activity, or which encourages or aids persons to undertake any unlawful activity, or of which the members undertake such activity; or

(ii) which has for its object any activity which is punishable under section 153A or section 153B of the Indian Penal Code (45 of 1860), or which encourages or aids persons to undertake any such activity, or of which the members undertake any such activity:

Provided that nothing contained in sub-clause (ii) shall apply to the State of Jammu and Kashmir

⁵⁶ *Id.* Section 7(4).

⁵⁷ *Id.* Section 11.

⁵⁸ *Id.* Section 17.

⁵⁹ *Id.* Section 21.

⁶⁰ *Id.* Section 24.

⁶¹ *Id.* Section 25(6).

⁶² *Id.* Section 26.

⁶³ *Id.* Section 30.

⁶⁴ *Id.* Section 43 F (1).

⁶⁵ *Id.* Section 43 F (2).

Disclaimer: While every effort is made to avoid any mistake or omission, this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification is being circulated on the condition and understanding that the publisher would not be liable in any manner by reason of any mistake or omission or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this casenote/ headnote/ judgment/ act/ rule/ regulation/ circular/ notification. All disputes will be subject exclusively to jurisdiction of courts, tribunals and forums at Lucknow only. The authenticity of this text must be verified from the original source.