2024 SCC OnLine Mad 6529 : (2024) 2 CTC 653 : (2024) 2 Mad LJ 439 : (2024) 1 LW (Cri) 427

In the High Court of Madras[†]

(BEFORE ANITA SUMANTH AND R. VIJAYAKUMAR, JJ.)

Karthick Theodore ... Appellant;

Versus

Registrar General and Others ... Respondents.

W.A.(MD) No. 1901 of 2021

Decided on February 27, 2024, [Reserved on : 29.09.2023]

Advocates who appeared in this case :

For Appellant : Mr. S. Jayavel

For Respondents : Mr. K. Samidurai - R 1 to R 3

No appearance - R 4

PRAYER : - Writ Appeal - filed under Clause XV of Letters Patent Act, to set aside the order passed in W.P.(MD) No. 12015 of 2021 dated 03.08.2021.

The Judgment of the Court was delivered by

ANITA SUMANTH, J.:—

BACKGROUND

The appellant/writ petitioner is aggrieved by order dated 03.08.2021, wherein the plea for a mandamus directing the Registrar General, Additional Registrar General and Registrar (IT-Statistics) (R1, R 2 and R 3 respectively) to redact his name and other identities from judgment dated 30.04.2014 in Crl.A. (MD) No. 321 of 2011 has been rejected. He had also sought a direction to Ikanoon Software Development Private Limited (R4) to reflect the redaction in its publication of the judgment in criminal appeal, which plea had also been rejected.

2. The appellant had faced criminal proceedings for offences under Sections 417 and 376 of the Penal Code, 1860 and had been convicted and sentenced by the trial Court by judgment dated 29.09.2011. The judgment was reversed by the High Court on 30.04.2011 in Crl.A.(MD) No. 321 of 2011 and the appellant was acquitted of all charges. The judgment has attained finality.

3. The appellant had, after acquittal, re-married and has three children. While so, the appellant had found, from a perusal of the High Court website, that the judgment dated 30.04.2011 revealed his personal details including details of his family that would reveal his identity.

4. He is aggrieved by the fact that such personal and intimate details of his life are available in public domain and claims protection by redaction of those details. This plea is based on his entitlement to privacy, particularly since his life has turned a new chapter and it is unnecessary for the private aspects of his past life to be open to public scrutiny.

5. The uploading of the unredacted judgment on the web portal has very significant repercussions in that, he was awaiting a visa for to travel to Australia that was denied by the authorities citing that criminal case. He thus made a request before R 4 that the judgment be taken down from the portal, to which it did not accede. He had thus approached this Court seeking the same relief which also came to be rejected. Hence, this writ appeal.

SUBMISSIONS OF THE APPELLANT

6. The arguments raised before the Writ Court are reiterated before us by Mr. Jayavel. He relies upon the judgment of the Supreme Court in *K.S. Puttaswamy* v. *Union of India*[1], wherein the right to privacy had been held to be an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution of India, enforceable in law.

7. The writ petitioner submits that the rights to be forgotten and of privacy are inherent in Article 21 of the Constitution. He assails the order of the writ court on the ground that redaction of name and identity are legal entitlements in light of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The uploading of judgments containing personal details triggers stereotypical ideas in the minds of the readers which continue long after the slur cast by the original judgment has been removed by the legal process.

8. Referring to the case of *XYZ Hospital*[2] he points out that the procedure of masking of personal and identifying details is not unknown to the Supreme Court which has been issuing such directions as an when deemed appropriate. In fact, in *Central Public Information Officer, Supreme Court of India* v. *Subhash Chandra Agarwal*[3] the Apex Court had held that Section 8(1)(f) of the Right to Information Act providing for Protection of the privacy of individuals is applicable to itself.

9. The writ Court has distinguished the decisions cited by the petitioner, referring to those specific instances where identity of victims has been protected either by statute or by the Court. The petitioner however makes a distinction between statutory protection afforded to children and victims of abuse, and the anonymity he seeks. In his case he has been declared innocent by the High Court and the State has accepted that judgment, as a result that the findings in the judgment have obtained finality. There is no justification for that slur to persist in the future as well.

10. The writ court, in denying the relief sought, has cited *Rup Ashok Hurra* v. *Ashok Hurra*[4] to state that no writ will lay against the superior courts. The petitioner makes a distinction between the relief sought for in *Hurra's case* (supra) which is one of certiorari as against the present prayer, which is a mandamus.

11. He further refers to the following cases in support of his case:

(i) *(Nameredacted)* v. *Registrar General, High Court of Karnataka*[5]

(ii) *X* v. *State of Maharashtra*[6]

SUBMISSIONS OF THE RESPONDENT

12. Per contra, the respondents, represented by Mr. K. Samidurai, emphasize upon the need for public access to judgments of the Court, relying on the judgment in *Swapnil Tripathi* v. *Supreme Court of India*[7]. For his part, the petitioner would emphasize that the prayer sought for by him would not militate against the need for public access to justice as no public purpose would be served by disclosing the details of the offending judgment.

13. Respondents also rely on *V. Swaminathan* v. *Registrar General, High Court of Madras*[8] wherein the Division Bench of this Court, vide decision dated 08.12.2021, rejected the plea for redaction of details of the Writ petitioner's daughter from a judgment dated 24.11.2016 in W.P. No. 20192 of 2013.

14. The objection raised by the Registry was that the writ petition was itself not maintainable and in stating so, reliance had been placed on the order of the Karnataka High Court in (*Name Redacted)* v. *Registrar General, High Court of Karnataka* (supra) and by the Kerala High Court in *XXX.* v. *Union of India*[9].

15. That writ petition has been dismissed with the Division Bench on the ground that the High Court is a Court of Record and in the absence of specific Rules, mandamus could not be granted. The objections raised by the Registry were accepted and the writ petition held not to be maintainable.

16. They refer to the decision in *R. Rajagopal* v. *State of Tamil Nadu*[10], where this Court has opined that the Rule of privacy is subject to the exception that publication becomes unobjectionable if it is based upon public records including court records.

17. Likewise, they refer to Section 327 of the Cr. P.C. that provides that Judicial Institutions should normally be open and transparent, such that the public would have access to both the courts and to their judgments. As far as the victims under POCSO cases are concerned, the States and Union Territories were directed to set up a one-stop centre in every district within one year of that judgment.

18. The Orissa High Court in *Subhranshu Rout @ Gugul* v. *State of Odissa*[11] also dealt with this issue while adjudicating upon an application under Section 439 of the Cr. P.C. The petitioner in that case had opened a fake facebook ID in the name of the informant, uploading objectionable photos of hers.

19. He sought bail and while dealing with that plea, the High Court held that information, once out in public domain, particularly in social media, is like tooth paste, impossible to put back in the tube. After referring to various judgments, both domestic and International in the context of privacy, the Court declined the relief of bail.

DISCUSSION

20. We have heard the detailed submissions of the parties and perused the records as well as the case law relied upon. The right to be forgotten was first recognized in French jurisprudence and referred to as *le droit à l'oubli.* The right was conferred upon convicts who had been released to help them make a fresh start in their lives, independent of their past by allowing them to seek erasure of their names from official databases.

21. The European Court of Justice in *Google Spain SL, Google Inc.* v. *Agencia Espannola de proteccion de Datos (AEPD), Mario Costeja Gonzalez*[12] allowed deletion of information which Mr. Gonalez had said was irrelevant but which continued to damage his reputation.

22. Coming home, the judgment in the case of *K.S. Puttaswamy* (supra) has settled the position that the right to privacy is an inalienable right, and one that is part of the Right to life enshrined in Article 21. Inter alia, the Bench has also dealt with the various components of the Right to privacy, including the Right to be forgotten.

23. The judgment is encyclopedic and renders superfluous the necessity to refer to the cases cited by the parties as they have been exhaustively referred to in that judgment. The Bench concludes in unison that the Right to Privacy is an inalienable right subject to the restrictions specified in Part III of the Constitution of India.

24. Specific reference may be made to paragraphs 615, 631 and 636 and paragraph 526 in the concurring opinions of Nariman J and Sanjay Kishan Kaul J. respectively, where the right to be forgotten has been discussed as follows:

> *Nariman, J.*
>
> .....
>
> *615. An issue like privacy could never have been anticipated to acquire such a level of importance when the Constitution was being contemplated. Yet, today, the times we live in necessitate that it be recognised not only as a valuable right, but as a right Fundamental in Constitutional jurisprudence.*

631. The impact of the digital age results in information on the internet being permanent. Humans forget, but the internet does not forget and does not let humans forget. Any endeavour to remove information from the internet does not result in its absolute obliteration. The foot prints remain. It is thus, said that in the digital world preservation is the norm and forgetting a struggle.

636. Thus, the European Union Regulation of 2016 has recognized what has been termed as 'the right to be forgotten'. This does not mean that all aspects of earlier existence are to be obliterated, as some may have a social ramification. If we were to recognize a similar right, it would only mean that an individual who is no longer desirous of his personal data to be processed or stored, should be able to remove it from the system where the personal data/information is no longer necessary, relevant, or is incorrect and serves no legitimate interest. Such a right cannot be exercised where the information/data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the Supra performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy.

Sanjay Kishan Kaul, J.

526. But this is not to say that such a right is absolute. This right is subject to reasonable regulations made by the State to protect legitimate State interests or public interest. However, when it comes to restrictions on this right, the drill of various Articles to which the right relates must be scrupulously followed. For example, if the restraint on privacy is over fundamental personal choices that an individual is to make, State action can be restrained under Article 21 with Article 14 it is arbitrary and unreasonable; and under Article 21 with Article 19(1) (a) only if it relates to the subjects mentioned in Article 19(2) and the tests laid down by this Court for such legislation or subordinate legislation to pass muster under the said Article. Each of the tests evolved by this Court, qua legislation or executive action, under Article 21 read with Article 14; or Article 21 read with Article 19(1)(a) in the aforesaid examples must be met in order that State action pass muster. In the ultimate analysis, the balancing act that is to be carried out between individual, societal and State interests must be left to the training and expertise of the judicial mind.

SUMMARY OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

25. The Digital Personal Data Protection Act, 2023 (in short 'DPDP Act') has received the assent of the President on 11.08.2023. It provides for processing of digital personal data in a manner that recognizes both the right of the individuals to protect their personal data, and the need to process such data for lawful purposes and for matters connected therewith or incidental thereto.

26. The writ Court had noted at the time when the impugned order was passed, that there had been no legislation in this respect as the Bill was yet to be passed. Today, as we have the benefit of the enactment, we outline below the scheme of the Act to understand better the scope of protection that it affords. Section 2 defines several relevant terms and 'data' is defined under Section (2)(h) as follows:—

> *'data' means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;*

27. The data protected is as between a data fiduciary and data principle and both terms are defined as follows:—

> *i) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;*
>
> *(j) "Data Principal" means the individual to whom the personal data relates and where such individual is—*
>
> *(i) a child, includes the parents or lawful guardian of such a child;*
>
> *(ii) a person with disability, includes her lawful guardian, acting on her behalf;*

28. *'Personal data'* is defined under clause (t) to mean any data about any individual who is identifiable by or in relation to such data and *'personal data breach'* means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to the personal data, that compromises confidentiality, integrity or availability of personal data.

29. There is another category referred to as 'Significant Data Fiduciary' which means any data fiduciary or class of data fiduciaries as may be notified by the Central Government under Section (10) of the Act.

30. The application of the Act is in the following manner:

> *3. Subject to the provisions of this Act, it shall—*
>
> *(a) apply to the processing of digital personal data within the territory of India where the personal data is collected—*
>
> *(i) in digital form; or*
>
> *(ii) in non-digital form and digitised subsequently;*

(b) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;"

31. Certain exemptions to the applicability of the Act are set out in clause (c) as follows:

(i) personal data processed by an individual for any personal or domestic purpose; and

(ii) personal data that is made or caused to be made publicly available by—

(A) the Data Principal to whom such personal data relates; or

(B) any other person who is under an obligation under law for the time being in force in India to make personal data available."

32. Chapter II containing Sections 4 to 10 sets out the obligations of Data Fiduciary. Section 4 states that a person may process the personal data of a Data Principal only in accordance with the provisions of the Act and for purposes that the Data Principal has consented or that are otherwise legitimate, meaning not expressly forbidden by law.

33. Section 5 states that every request made seeking consent to a Data Principal shall be accompanied by or preceded by a notice from the Data Fiduciary informing her of the personal data in possession of the Data Fiduciary and the purpose for which it is proposed to be processed. She is also to be intimated of her rights under the Act, particularly Section 6(4) and 13 and the manner in which she may complain, if aggrieved by the use of personal data before the Board.

34. Section 6 requires consent given by the Data Principal to be free, informed, specific, unconditional and unambiguous. Once the consent is given, it signifies agreement to the processing of her personal data solely for the purposes it has been collected.

35. Section 7 adumbrates the uses for which personal data of a Data Principal may be utilized being

(a) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.

(b) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where—

(i) she has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(ii) such personal data is available in digital form in, or in nondigital form and digitised subsequently from, any database,

register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government, subject to standards followed for processing being in accordance with the policy issued by the Central Government or any law for the time being in force for governance of personal data.

(c) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

(d) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(e) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

(f) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

(g) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;

(h) for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

Explanation.—For the purposes of this clause, the expression "disaster" shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005; or

(i) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

36. Section 8 casts responsibility on the Data Fiduciary for full compliance with the provisions of the Act and the Rules and makes it clear that it is to carry out its duties under the Act in a responsible manner. Any assistant appointed for that purpose would only be under a valid contract. The use of the data by the Data Fiduciary should be appropriate, accurate and consistent.

37. The Data Fiduciary is expected to protect the personal data in its possession or in its control putting in necessary safety measures to prevent data breach. Intimation is to be given to the Board and to the affected Data Principal in the event of a data breach. Section 8(7) is important to this case, as it provides for erasure of personal data. Sub-clause (7) reads as follows:

> *(7) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—*
>
> *(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and*
>
> *(b) cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for processing to such Data Processor.*

38. The purpose referred to in Section 8(7)(a) shall be deemed to no longer be served, if the Data Principal does not approach the Data Fiduciary for performance of the specified purpose and exercise of her rights in relation to such processing for a specified time period to be stipulated by Data Fiduciaries.

39. The Data Fiduciary is expected to publish the contact information of a Data Protection Officer who would be liasoning with the Data Principal in regard to the processing of the personal data. A Data Fiduciary is also expected to establish an effective mechanism to redress the grievance of the Data Principal.

40. Section 9 deals with the processing of personal data of children. Section 10 imposes obligations upon a significant Data Fiduciary and the Central Government can notify a Data Fiduciary or class thereof as a significant Data Fiduciary on the basis of an assessment of various factors including the following:

(a) the volume and sensitivity of personal data processed;

(b) risk to the rights of Data Principal;

(c) potential impact on the sovereignty and integrity of India;

(d) risk to electoral democracy;

(e) security of the State; and

(f) public order.

41. Once designated as a significant Data Fiduciary, such entity would have to appoint a Data Protection Officer who shall represent it for the purposes of the Act, be responsible to the persons in management of that significant Data Fiduciary and be the point of contact for the grievance redressal mechanism under the Act. The significant Data Fiduciary should also appoint an independent Data Auditor to carry out data of the audit and a periodic data protection

impact assessment in regard to the processing of the large quantities of data in its possession.

42. Chapter III sets out the rights and duties of a Data Principal and contains Sections 11 to 15. Sections 11 and 12 vest the rights of obtaining from the Data Fiduciary the summary of personal data as well as the identities of all other Data Fiduciaries and Data Processors with whom her personal data has been shared. The latter is inapplicable where such sharing was pursuant to a request made by another Data Fiduciary for the purpose of prevention, detection or investigation of cyber offences or cyber incidents or for the prosecution or punishment of offences.

43. The Data Principle has the right of correction, completion, updation and erasure of personal data under Section 12. Such erasure is to be carried out upon request unless the retention of the same were to be necessary for the specified purpose of compliance with any law for the time being in force. The duties to be performed by a Data Principal are set out under Section 15.

44. The special provisions set out under Chapter IV include Sections 16 and 17. Section 16 vests power in the Central Government to, by Notification, restrict transfer of personal data by a Data Fiduciary for processing anywhere outside India. It is tempered by sub-section (2) which states that the restriction will not apply if the law outside India provides for a higher degree of protection than what is available within the Country.

45. Section 17 states that the provisions of Chapter II, except Section 8(1) and 8(5) and Chapter III and Section 16 would not apply in certain specified situations as below:

> *17. (1) The provisions of Chapter II, except sub-sections (1) and (5) of section 8, and those of Chapter III and section 16 shall not apply where—*
>
> *(a) the processing of personal data is necessary for enforcing any legal right or claim;*
>
> *(b) the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function;*
>
> *(c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India;*
>
> *(d) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in*

India;

(e) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force; and

(f) the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.

46. Thus, the only provisions that would be applicable to a Court, Tribunal or anyone entrusted with the purpose of rendition of judicial or quasi judicial functions (per Clause (b) of sub-section (1) of Section 17) would be Section 8(1) and 8(5), extracted below, the provisions contained in Chapter III, being Rights and Duties of Data Principal and Section 16, and it is exempt from all other obligations as adumbrated under Chapter II:

8 (1) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.

8 (5) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

47. The important ramification of the insulation as contained in Section 17(1)(b) is that the Section 8(7), that provides for erasure of personal data is now rendered inapplicable to Courts, tribunals and quasi-judicial authorities. The impact of this insulation, specifically upon the Data Principals have been addressed in the paragraphs to follow.

48. Chapter III, containing Sections 11 to 15 contains the rights and duties of a Data Principal and Section 16, being the power of the Central Government to transfer data, is extracted below:

16. (1) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

(2) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

49. Under Chapter V, a Data Protection Board of India has been set up which provides for a Board with a Chairperson and Members. Chapter V deals with various details relating to the constitution of the board, their terms of reference and other matters.

50. Chapter VI deals with the powers, functions and procedure to be followed by the Board and contains Sections 27 and 28. The Board is to look into complaints of personal data breaches and Section 28 states that as far as practicable, the Board shall function as a digital office.

51. Sections 29 to 32 provide for appeals and resolution of disputes by Alternate Dispute Mechanisms coming under Chapter VII. Chapter VIII dealing with Sections 33 and 34 deal with the imposition of penalties and adjudication of matters. Chapter IX deals with Miscellaneous matters, such as making of Rules, bar against filing of Suits, an omnibus grant power to the Central Government requiring the Board, Data Fiduciary or Intermediary to provide such information as it may call for etc.

52. In Section 44, there are provisions for consequential amendment of other enactments and sub-section (3) assumes importance. Section 8(1)(j) of the Right to information Act (RTI Act) now reads *information which relates to personal information the disclosure of which has no relationship to any public activity or interest or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer of the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information'.* This sub-section will now stand substituted to read *'information which relates to personal information'*. With this substitution, the balance that was sought to be achieved between personal and public interest under the RTI Act will stand diluted. There is a direct consequence of this position on the functioning of the Courts as Data Fiduciaries that we address in the paragraphs to follow.

APPLICATION OF THE DPDP ACT TO THE COURTS

53. The scope, thrust and object of the DPDP Act is to regulate the collection of data and, simultaneously, protect personal data. Achieving such a balance is critical to a society that straddles a transparent and open system of working with safeguards and measures in place for the protection of personal data. A decision on the applicability of the Act or otherwise must thus, in our considered view, lean in favour of inclusion rather than exclusion.

54. Section 3(c) expressly states that the Data Protection Act shall not apply to (a) the Data Principal to whom such personal data relates or (b) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available. The term 'person' used in Section 3(c)(ii)(B) encompasses an individual, a hindu undivided family, a Company, a firm, an association of persons or a body of individuals, whether incorporated or not, the State and every artificial juristic person not falling within any of the preceding sub-clauses. While the High Court is an artificial juristic person, there is no obligation cast upon the Courts to make personal data publicly available.

55. The exemption contained under Section 3(c)(ii)(B) contains two limbs. Firstly, the entity must be a '*person'* as understood under the provisions of the DPDP Act, which the High Court is, and secondly, there must be an obligation for disclosure of personal data held by it. In the present case, the second limb is not satisfied.

56. A Constitutional Court, such as the High Court is a Court of Record and is expected to hold in its possession such data as constitutes its 'record', in perpetuity. The decision and discretion as to whether such data is to be made publicly available is fully available with the Institution itself, and such decisions are taken consciously and carefully.

57. Courts cannot be compelled to make available any information in public domain subject to the compulsions imposed by the RTI Act, and, in the interest of public access to justice and courts, such discipline is self-imposed. Courts are expected to perform a fine balancing act between aggregation of data required to perform its functions and protection of personal data so collected.

58. Efforts are also ongoing administratively within the Institution to construct and formalize a Policy for Privacy and Data Protection, applicable pan India. and this process is all the more enabled with the enactment of the DPDP Act. The Act contains the structure that may be put in place to address and redress such concerns and can be moulded to suit the unique specificities of the Courts. Till such time a policy is put in place, it becomes incumbent on every High court to devise a mechanism by which requests of the nature put forth by the writ appellant, are addressed and redressed.

59. Courts have, time and again, addressed this issue, taking the initiative to intervene and protect the victims in various situations and circumstances. In *Nipun Saxena* v. *Union of India*,[13], the Hon'ble Supreme dated 11.12.2018 Court considered how and in what manner, the identity of adult victims of rape and children who are victims of sexual abuse should be protected.

60. They refer to Section 228A introduced in the Indian Penal Court vide Amendment Act No. 43 of 1983 with effect from 25.12.1983 that provided for certain guidelines to be followed in the disclosure of identity of the victims of certain offences. In the case of *X* v. *State of Maharashtra* as well, the Supreme Court has directed the Registry to mask the name of the informant pending adjudication of her case.

61. As the writ petitioner points out, he does not seek statutory protection but rather the exercise of discretion by the Court for enforcement of his fundamental right of erasure. The 'Right to be forgotten', or rather the 'Right to be remembered well', cannot be denied to a person if the facts and circumstances so commend it.

62. The concerns of privacy so acutely felt now, are a feature of the Internet age. The uncontrolled and unbridled dissemination and availability of information that have been noted in the judgment in *K.S. Puttaswamy* necessitate such discretion in appropriate circumstances and if the Court were certain that the claim of the person is indeed justified. We are thus of the considered view that granting the relief of masking/redaction of information from certified copies that are issued for public circulation must be enabled in appropriate situations.

63. What those situations are, would be a matter of consideration on a case to case basis. The Right to Privacy of an individual would have to be finely balanced with the right of the citizen 'to know'. It is in these circumstances that a streamlined structure as contemplated under the Act would come a long way in providing a structured remedy to an aggrieved individual.

64. Courts have wide discretion in deciding whether disclosure must be preferred to redaction. Such discretion can be exercised either at the request of the party seeking redaction or in appropriate cases even where such request has not been made by the party, suo motu by the Court. Courts are sensitive to the position that, many a time, litigants may be unaware of the protection/privacy that they are entitled to and in such instances, would take it upon themselves to afford such privacy in appropriate cases and even where the party has not specifically sought such protection. Such occasions may arise in the most unexpected scenarios.

65. One of us (Anita Sumanth, J) had occasion to deal with a batch of matters relating to a challenge to income tax assessments pursuant to search and survey under the provisions of the Income Tax Act, 1961. One of the arguments in support of the challenge to the search conducted under Section 132 of the Income Tax Act was that there had been unwarranted and illegal intrusion into the homes of the petitioners by the officers of the Income Tax Department.

66. The petitioners had referred to one of the family members, a young girl, having suffered medical ailments on account of the

extended hours of search and the lack of adherence to basic tenets of human rights. They alleged that the family member was prone to medical history of seizures caused by disturbed sleep patterns, stress and lack of timely food. These facts were part of the record including the name and medical history of the family member.

67. While this aspect of the matter, that is, the procedure followed in carrying out the search, had necessarily to be taken into account in deciding the veracity or otherwise of the search itself, there was no need to reveal the personal details of the family member itself as it was extraneous to the legal issue. It would thus suffice to outline the incident without any necessity for minute and private details, such as the name of the family member, name of treating doctor, name of the hospital and details of medical condition.

68. There was no request by the party for redaction or masking. But in dealing with the issue, the private details were withheld on a careful consideration of personal interest vis-a-vis private interest (see decision in *Chandran Somasundaram* v. *Principal Director of Income Tax, Coimbatore*[14]). In today's reality of enhanced and often times, cumbersome visibility, the Court is vested with sufficient inherent powers to mast/redact personal information where necessary, and does not have to seek support from external sources. The strength and sensitivity of a Constitutional Court, would suffice in this regard.

69. The grievance of an individual who wishes to invoke the right of erasure can now be address in a systematized manner. True, the provisions of Section 8(7) of the DPDP Act dealing with the Right of erasure have not been extended to the Courts by virtue of Section 17 of the DPDP Act. However, there is nothing that prevents the Courts from providing such succor or solace to deserving persons upon our being so convinced, and it is left for the Courts to sift the facts of each case and decide on such erasure/redaction.

70. Section 12(3) provides that personal data may be erased unless retention of the same is necessary for specified purpose or for compliance with any law for the time being in force. The definition of ‘data’ under Section 2(h) means *a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means*.

71. ‘Digital Personal Data’ is defined under Section 2(n) to mean personal data in digital form. An order of the Court would thus constitute ‘data’ in satisfaction of the definition under Section 2(h) and such order, when available in a digital form containing personal data, inter alia, would constitute digital personal data. ‘Personal Data’ is defined under Section 2(t) to mean ‘*any data about an individual which*

is identifiable by or in relation to such data.'

72. Essentially the order under challenge, contains three fold reasoning to reject the plea for mandamus (i) that a writ cannot lie against the judgment or order passed by it as that would tantamount to a High Court issuing a writ against itself (ii) that the High Court is a Court of Record and is entitled to preserve its record for perpetuity (iii) based on the principle of open courts and justice, the 'right to be forgotten' is an exception to the principle of open justice that either has to be statutorily provided for or specifically directed by the Supreme Court.

73. Adverting to the first point, we do not agree that the petitioner seeks issuance of a writ against the High Court. To our mind, there is a distinction between a prayer where the relief sought is as against the Institution itself and the present case where the petitioner seeks protection of his privacy by way of redaction or masking of personal/private details rendered irrelevant by passage of time but which continue to haunt him. In fact, redaction or masking is not unknown to the Courts and we cite below two such instances.

74. In the case of *X* v. *State of Maharashtra*[15] the Hon'ble Supreme Court considered the case of the appellant who had claimed to be exposed to the horrors of the casting couch syndrome. Appeals had been filed challenging orders of the Bombay High Court allowing anticipatory bail applications filed by the respondent. While quashing the orders and cancelling the bail bonds, the Registry was directed suo motu by the Bench to protect the identity of the appellant and take immediate steps to redact the name of the appellant from the records.

75. A general direction was also issued to ensure that in sensitive matters, if the name of the appellant/prosecutrix was revealed, the matter be returned to the counsel for redacting the name before clearing the same and listing before the Court. Another instance is the Karnataka High Court in the case of *(Name Redacted)* v. *Registry of the High Court of Karnataka* (supra) referred to in paragraph 15 above.

76. On the second point, the High Court, under Article 215 of the Constitution of India is a Court of Record. In the course of the services that it renders, it becomes a repository of a wide range of information, a significant portion of which comprises personal information of individuals. The argument that the High Court as a Court of Record is entitled to preserve the original record in perpetuity, is unassailable. However, the sanctity of an original record is not diluted in any way, if a public reflection of that record is moderated to preserve the privacy of the person to whom that record pertains.

77. Thus, while the records of the Court remains sacrosanct and untouched, all that is called for is a direction to redact or mask the

personal details from the judgment when published/uploaded, such that the identity of the parties remains private. Undoubtedly, the parties to the litigation are entitled to certified copies of the unredacted and complete judgment. Under the Madras High Court Appellate Side Rules, Order XII deals with issuance of certified copies. Rule 1 bars the entitlement of any person to a copy of Judges' notes or minutes, correspondence not strictly judicial and confidential correspondence.

78. Rule 2 states that any party to a proceeding shall be entitled to obtain copies of judgments, decrees or orders made or of any documents filed or exhibited in such proceeding on payment of charges in the manner prescribed under those rules. Rule 3 states that any person who is not a party to a proceeding, requiring copies of judgments, decrees or orders made or of any documents filed or exhibited in such proceeding, may apply to Court for grant of such copies by a duly stamped petition.

79. Once a party applies to the Court for grant of copies, an application will have to be filed in terms of Rule 4 for obtaining such a copy. The proviso to Rule 4 as applicable prior to substitution by R.O.C. No. 4282-A/2010/F1 dated 22.12.2010 reads as follows:

> *'Provided that, in cases of doubt whether the copy applied for should be furnished, the application shall be placed before the Registrar for his decision. If the application is refused by the Registrar, it shall be returned to the applicant with the order of the Registrar endorsed on it'.*

80. Post its substitution the proviso reads thus:

> *Provided that, in cases where issuance of certified copies to the third parties is restricted by any judicial order to maintain secrecy and privacy the Registrar shall refuse the application.*

81. Clearly, the Rules have been drafted in contemplation of privacy and protection of private interests, even several decades ago. It is thus open to any person who is a party to the proceedings to approach the Court and obtain an order for maintenance of secrecy and privacy and in respect of matters where such judicial order was obtained, the order would have to be transmitted to the Registry, such that the Registry could refuse or reject applications by third parties for copies.

82. Order XI of the Madras High Court Original Side Rules provides for a party to a suit or a matter to be entitled to obtain copies of judgments, decrees, orders made, documents or exhibits on payment of charges prescribed and Order XIV Rule (v) enables applications by strangers to a suit for leave to inspect the records and for obtaining copies of the records. The Rules thus do enable protection and privacy of litigants though the ultimate discretion in either accepting or rejecting a request remains with the Court.

83. On the aspect of open Courts, The Kerala High Court in *Vysakh K.G.* v. *Union of India*, had declared that the claim for protection of personal information based on the right to privacy cannot co-exist in an Open Court justice system. The following directions were issued:

> *64. In summation, we hold as follows:*
>
> *i. We declare that a claim for the protection of personal information based on the right to privacy cannot co-exist in an Open Court justice system.*
>
> *ii. We hold that right to be forgotten cannot be claimed in current proceedings or in a proceedings of recent origin. It is for the Legislature to fix grounds for the invocation of such a right. However, the Court, having regard to the facts and circumstances of the case and duration involved related to a crime or any other litigation, may permit a party to invoke the above rights to de-index and to remove the personal information of the party from search engines. The Court, in appropriate cases, is also entitled to invoke principles related to the right to erasure to allow a party to erase and delete personal data that is available online.*
>
> *iii. We declare and hold that in family and matrimonial cases, arising from the Family Court jurisdiction or otherwise and also in other cases where the law does not recognise the Open Court system, the Registry of the Court shall not publish personal information of the parties or shall not allow any form of publication containing the identity of the parties on the website or on any other information system maintained by the Court if the parties to such litigation so insist.*
>
> *iv. We hold that the Registry of the High Court is bound to publish privacy notices on its website in both English and Vernacular languages.*

We are given to understand that a review application is pending as against the order.

84. The open justice system is dealt with in detail in the case of *Swapnil Tripathi* v. *Supreme Court of India*. Three Judges of the Hon'ble Supreme Court, noting that generally criminal and civil Courts in India are open Courts, opined that technology has made it possible for Courts to literally be open in the sense of removing infrastructural restrictions and logistical issues.

85. Indeed, the phenomenon of open Courts has literally brought justice as well as the justice dispensation system to the doorsteps of citizens. There has however, to be a fine balance between the concept of open justice and that of the privacy of the litigant. The fact that privacy is an inalienable and undeniable facet of the right to life and

dignity is too well settled now. That apart, the right to erasure is also now statutorily enshrined in the DPDP Act.

86. While the appellant relies on the judgment in the case of *K.S. Puttaswamy*, the respondent would rely on the judgment in the case of *Swapnil Tripathi*. In our considered view and having studied both the judgments carefully, we do not believe that the same militate at any level whatsoever. A careful balance has to be achieved between the concept of Open Court and Open access justice, and the cry for privacy. There could be no totalitarian application of either one concept as that would defeat the purpose of both equally valid concepts.

87. Being a service institution committed to serving the cause of justice, the Courts cannot close their eyes to the concerns of privacy and the right that enure in the litigations to leave behind parts of their past which are no longer relevant. This, in our view, would be a proper understanding and reconciliation of the ratio of the judgments in *Swapnil Tripathi* and *K.S. Puttasamy*, balancing the concept of open Court/open justice on the one hand and privacy concerns of a citizen, on the other.

88. Thus, even sans the benefit of the DPDP Act, which is yet to be notified, we are of the view that the inherent powers of the Court would extend to issuing Mandamus as sought for. The Writ Petitioner is entitled to the relief sought on the facts and circumstances of this case.

89. The Writ Court has also expressed helplessness in passing '*orders and judgments in acquittal due to slipshod investigation, dishonest witnesses and lack of an effective witness protection system. This Court honestly feels that our criminal justice system is yet to reach such standards where Courts can venture to pass orders for redaction of name of an accused person on certain objective criteria prescribed by rules or regulations'.*

90. The question is as to whether the exercise of discretion by Courts is circumscribed by the perfection or otherwise of a system in which we are, but one stakeholder. True, Courts must do everything in their power and strive to perfect the system. However, we do believe that the fallibility or vulnerability of the criminal justice system must not stand in the way of rendition of justice elsewhere, if, when, and where it is called for.

91. In the present case, there is no dispute in that the judgment in Crl.A. (MD) No. 321 of 2011 has attained finality. In that judgment, the Bench states categorically '*In the result, I hold that the appeal should be allowed and the accused acquitted. I am not giving any benefit of doubt to the accused and acquitting him, but I am holding that the accused has disproved the prosecution case and has earned this acquittal.'* The acquittal is thus full, complete and unconditional.

92. The writ petitioner has moved on and there is no public interest

in retaining, as part of public record, a chapter of his life that has no relevance now. The fact that the 'principle of fresh start' has been statutorily enshrined under the Juvenile Justice (Care and Protection of Children) Act, 2015 cannot lead to the conclusion that adults are not entitled to the same.

CONCLUSION:

93. Thus, there is a direction to R 4 to take down the judgment in Crl.A. (MD) No. 321 of 2011 dated 30.04.2014 forthwith. There is a further direction to R 1 to R 3 to redact the name and other details of the Writ Petitioner relating to his identity from judgment dated 30.04.2014 in Crl.A.(MD) No. 321 of 2011 and ensure that only the redacted judgment is available for publication or for uploading. Needless to say, the full and unredacted version of the judgment shall continue to be part of the record of the Court.

94. This Writ Appeal is allowed and connected miscellaneous petitions are closed without there being any order as to costs.

———

† Madurai Bench

[1] (2017) 10 SCC 1

[2] ((1998) 8 SCC 296)

[3] [(2020) 5 SCC 481]

[4] [(2002) 4 SCC 388]

[5] (2017 SCC OnLine Kar 424)

[6] (2023 SCC OnLine SC 279)

[7] ((2018) 10 SCC 639)

[8] (decision dated 08.12.2021 in W.P. No. SR.73910 of 2021)

[9] WP(C). No. 9982 OF 2021(W) dated 19.04.2021

[10] ((1994) 6 SCC 632)

[11] 2020 SCC OnLine Ori 878

[12] Case (C-131/12 May 13, 2014) Court of Justice of the European Union

[13] W.P.(C) 565 of 2012

[14] (2023) 450 ITR 188

---

[15] 2023 SCC OnLine SC 279