DigitalRightsFoundation
"KNOW YOUR RIGHTS"

ڈیٹا پرائیویسی کتابچہ برائے پالیسی سازوں

فہرست مضامین

کلیدی مخففات کی لغت —— 01
اغراض و مقاصد —— 02
تعارف —— 02
پرائیویسی کے اصول —— 03
ڈیٹا کسے کہتے ہیں؟ —— 05
پرسنل ڈیٹا کسے کہتے ہیں؟ —— 05
پرائیویسی کیا ہے؟ —— 07
رضامندی کسے کہتے ہیں؟ —— 08
سنِ بلوغت اور نا بالغ پن کی عمر کیا ہے؟ —— 09
نا بالغان کیلئے خصوصی اقدامات —— 09
نجی اور عوامی آن لائن مقامات میں فرق —— 12
ڈیٹا پروسیسرز اور ڈیٹا کنٹرولرز کون ہوتے ہیں؟ —— 12
ڈیٹا کا تحفظ کیوں ضروری ہے؟ —— 13
ڈیٹا خود مختاری —— 13
تکنیک کی بنیاد پر صنفی تشدد و زیادتی (TF-GBV) —— 14
پرائیویسی پر پاکستانی فقہ —— 15
ڈیٹا مالکان کے حقوق —— 16
ڈیجیٹل شناخت کے مضمرات —— 18
بڑھتی ہوئی ڈیجیٹائزیشن اور پرائیویسی پر اس کے اثرات —— 19
حاصل کلام —— 21
حوالہ جات —— 32

ہمارے متعلق

ڈیجیٹل رائٹس فاؤنڈیشن (ڈی ۔آر۔ایف) پاکستان کا ایک رجسٹرڈ شدہ غیر حکومتی تحقیقاتی ادارہ ہے ۔ اس کا قیام 2012 میں عمل میں آیا۔ ڈی ۔آر ۔ ایف ، ڈیجیٹل گورننس، جمہوری طور طریقوں اور انسانی حقوق کی حمایت کرتے ہوئے معلومات برائے کمپیوٹر ٹیکنالوجیز پر نظر رکھتا ہے۔ ڈی ۔آر۔ ایف خاص طور پر خواتین پر ہونے والے آن لائن زیادتی کے خلاف، ڈیٹا کی حفاظت، پرائیویسی یعنی رازداری، خواتین کی حصہ داری اور آن لائن آزادئ رائے کے راستے میں آنے والے مسائل پر کام کرتا ہے۔ ہمارا ادارہ انسانی حقوق کی راہ میں حائل ہر قسم کے تعصب اور جنسی تفریق اور ہر طرح کی آن لائن سنسر شپ خواہ وہ آن لائن ہوں یا آف لائن ہوں ان کی مخالفت کرتا ہے۔

مزید معلومات کیلئے

www.digitalrightsfoundation.pk

اعترافات

اس معلوماتی مواد کی تصنیف و تحریر میں حصہ لینے والوں میں زینب درانی، انعم بلوچ اور مناہل فاروق شامل ہیں جب کہ سیرت خان کی جانب سے اس تحریری مواد کی ایڈیٹنگ کی گئی ہے۔ اس کو ڈیزائن کرنے میں احسن زاہد اور طلحہ عمر شامل ہیں۔

اعلان دستبرداری

اس مواد کی اشاعت میں درستگی کو یقینی بنانے میں ہر ممکن کوشش کی گئی ہے تاہم مصنفین اور ادارہ ہذا کسی بھی غلطی یا بھول چوک کیلئے ذمہ داری قبول نہیں کرتے کیونکہ ارادتاً کوئی بھی غلطی نہیں کی جاتی۔ تاہم، درست معلومات کی فراہمی کیلئے حتی الوسع ہم اپنے کام کو مزید بہتر کرنے کیلئے کوشاں رہیں گے۔

کلیدی مخففات کی فہرست

یو ڈی ایچ آر: یونیورسل ڈیکلریشن آف ہیومن رائٹس۔ 1948میں اپنایا گیا، یو ڈی ایچ آر اقوام متحدہ کے اولین دستاویزات میں سے ایک ہے جس میں "بنیادی انسانی حقوق" کو دنیا بھر میں محفوظ کرنے کے اصول طے کیے گئے۔ یہ دستاویز تقریباً ستر سے زیادہ انسانی حقوق کے معاہدوں کی بنیاد بنی، جو آج عالمی اور علاقائی سطح پر مستقل طور پر نافذ ہیں اور ان کے دیباچوں میں اس کا حوالہ موجود ہے۔[1]

سی ای ڈی اے ڈبلیو: خواتین کے خلاف ہر قسم کے امتیاز کے خاتمے کا کنونشن۔ 1979میں اپنایا گیا، سی ای ڈی اے ڈبلیو "خواتین کے حقوق کے عالمی منشور" کے طور پر بیان کیا جاتا ہے۔ یہ دیباچہ اور30 شقوں پر مشتمل ہے، جس میں خواتین کے خلاف امتیاز کی تعریف کی گئی ہے اور اسے ختم کرنے کے لیے قومی سطح پر اقدامات کا ایجنڈا طے کیا گیا ہے۔[2]

آئی سی سی پی آر: شہری اور سیاسی حقوق کا بین الاقوامی معاہدہ۔ 1966 میں اپنایا گیا، آئی سی سی پی آر ایک بین الاقوامی معاہدہ ہے جو سب کے لیے حقوق اور آزادیاں فراہم کرنے کا عہد کرتا ہے، جس میں زندگی کا حق، آزادی، قانون تک مساوی رسائی، تشدد، غلامی اور امتیاز سے تحفظ شامل ہیں۔[3]

این سی پی ڈی پی: نیشنل کمیشن فار پرسنل ڈیٹا پروٹیکشن۔ این سی پی ڈی پی حکومتِ پاکستان کی جانب سے 2023 کے پرسنل ڈیٹا پروٹیکشن بل کے تحت قائم کیا گیا ایک نگران ادارہ ہے، جس کا مقصد پاکستانی شہریوں کی ڈیٹا پرائیویسی کا تحفظ کرنا ہے۔[4]

اغراض و مقاصد

اس کتابچے کے ذریعے ہمارا مقصد پاکستانی پالیسی سازوں کو وہ وسائل فراہم کرنا ہے جو انہیں بنیادی انسانی حقوق کے اصولوں، ڈھانچوں اور بہترین بین الاقوامی طریقوں کو سمجھنے میں مدد دیں، تاکہ انہیں پاکستان میں پرائیویسی کے حق اور ذاتی ڈیٹا کے تحفظ جیسے اہم تصورات سے متعلق قانون سازی نافذ کرنے میں شامل کیا جا سکے۔

تعارف

یونیورسل ڈیکلریشن آف ہیومن رائٹس (یو ڈی ایچ آر)[5] ایک ایسی بنیادی دستاویز ہے جو کہ 1948 میں ترتیب دی گئی یہ تمام اقوام اور تمام افراد کے لیے موضوع ہے. یو ڈی ایچ آر کے بارہویں آرٹیکل کے مطابق ذاتی رازداری کے حق یعنی پرائیویسی کا شمار انسان کے بنیادی 30 حقوق میں ہوتا ہے۔

پاکستان کے تناظر میں پاکستانی آئین[6] کے آرٹیکل 14 کے مطابق انسانی عظمت اور اس کی ذاتی رازداری کی بے حرمتی ممکن نہیں۔

ذاتی زندگی کی رازداری ایک بنیادی حق ہے اور اس پر کسی بھی قسم کا سوال اٹھانا بے بنیاد کہلائے گا ۔

ڈیجی ٹائیزیشن کو مختلف نظریوں سے دیکھا جائے تو اندازہ ہوتا ہے کہ اس نے تمام شعبہ زندگی کو متاثر کیا ہے ۔آن لائن اور آف لائن رہنے کے لا متناہی سلسلے نے ایسے خطرات کی نشاندہی کی ہے جو کہ ایک جگہ سے دوسری جگہ انتہائی آسانی سے پہنچ سکتے ہیں ۔ہماری آن لائن زندگی اور ہماری اصلی زندگی ایک دوسرے سے زیادہ مختلف نہیں ہے ان تمام باتوں کے پیش نظر اپنی ذاتی معلومات کی حفاظت آج کے دور میں ایک ترجیحی مسئلہ ہے پاکستان میں ڈیٹا کی حفاظت کے لیے باقاعدہ طور پر کوئی قانون موجود نہیں ہے ۔البتہ 2023[7] میں منسٹری آف انفارمیشن اور ٹیلی کمیونیکیشن نے ایک پرسنل پروٹیکشن بل متعارف کروایا تھا جس کو جلد ہی قانونی شکل دی جائے گی یہ کتابچہ اس بل کے تحت ان عناصر پر روشنی ڈالے گا جو کہ ڈیٹا کی حفاظت کے لیے ضروری ہے۔

پرائیویسی کے اصول

پاکستان کی بین الاقوامی ذمہ داریوں کے مطابق ذاتی ڈیٹا کے تحفظ پر ایک جامع، حفاظتی اور مضبوط فریم ورک درج ذیل اصولوں کے مطابق ہونا چاہیے :

- **اہم اصطلاحات کی وضاحت:** مسودے کے کچھ حصے ابہام پیدا کرتے ہیں، جیسے کہ 'قومی مفاد' (دفعہ 9(1)): سیکیورٹی کی ضروریات) یا 'قومی سلامتی' (دفعہ 32 اور34) کی تعریفیں۔ مسودے میں ایسی وسیع طور پر تعریف شدہ اصطلاحات کا ذکر کیا گیا ہے جیسے 'جائز مفاد' (دفعہ 2(یو))اور 'عوامی مفاد' (دفعہ 2(ایف ایف)) اسی طرح، 'انتہائی اہم ذاتی ڈیٹا' کی اصطلاح ابھی تک غیر واضح ہے اور اس کے ساتھ کوئی وضاحت نہیں جڑی ہوئی۔

  بل کا مسودہ تعریفیں بنانے اور اصطلاح میں ہم آہنگی فراہم کرنے کے لیے این سی پی ڈی پی پر بہت زیادہ انحصار کرتا ہے۔

- **انسانی حقوق کو اولیت دینا:** بل انسانی حقوق کو اولین ترجیح دینے میں ناکام ہے، جس سے قانون کے غیر مساوی اطلاق کا خطرہ ہے۔ اس مسئلے کو حل کرنے کے لیے یہ ضروری ہے کہ اہم اصطلاحات، تعریفیں اور عملدرآمد کے پروٹوکول عالمی انسانی حقوق کے معیارات کے مطابق ہوں۔ بنیادی توجہ ان کمیونٹیز کے تحفظ پر ہونی چاہیے جو کمزور ہیں، جن کا ڈیٹا خاص طور پر خطرے میں ہے، اور یہ عالمی ڈیٹا تحفظ کے بہترین طریقوں کے مطابق ہونا چاہیے۔ ذاتی ڈیٹا کو ایک قیمتی اور حساس مال سمجھتے ہوئے، عالمی اور انفرادی سطح پر اس کا تحفظ ضروری ہے۔ حکومتی ڈھانچے کو اس نقطہ نظر کو ترجیح دینی چاہیے تاکہ مساوی تحفظ یقینی بنایا جا سکے۔

- **کمزور گروپوں کی پرائیویسی کے تحفظ پر زیادہ توجہ:** پاکستان کا سی ای ڈی اے ڈبلیو، آئی سی سی پی آر کی توثیق اوراس کے یو ڈی ایچ آر کی رکن ریاست کے درجہ کی حیثیت سے اس کے قانون، پالیسی سازوں اور حکومت پر یہ ذمہ داری عائد ہوتی ہے کہ وہ ایسے اقدامات، قوانین اور پالیسیز وضع کریں جو نابالغوں، خواتین، صنفی اور مذہبی اقلیتی گروپوں کے ذاتی ڈیٹا کی حفاظت کے حوالے سے زیادہ تحفظ فراہم کریں اور اس کی خلاف ورزی سے پیدا ہونے والے نقصان کو کم کریں۔

- **شفافیت اور شمولیت:** قوانین اور پالیسیوں کا بنانا بذات خود ایک جمہوری عمل ہے کیونکہ یہ پوری آبادی کو متاثر کرتا ہے، اس لیے ایک جامع اور واضح مشاورت کا عمل اپنانا ضروری ہے، تاکہ اہم ڈھانچوں کا تعین کرتے وقت تمام فریقین کو بروقت اور کھلے طریقے سے شامل کیا جا سکے۔

- **نفاذ کا خود انحصار اور خود مختار ادارہ:** ذاتی ڈیٹا کے تحفظ کے لیے نیشنل کمیشن فار پرسنل ڈیٹا پروٹیکشن (این سی پی ڈی پی) جو کہ پی ڈی پی بی کے تحت متعلقہ ادارہ ہے، کو تمام معاملات، چاہے وہ انتظامی معاملات ہوں یا ملازمین اور افسران کی تقرری کے حوالے سے ہوں، وفاقی حکومت کی نگرانی اور اثر و رسوخ سے آزاد ہونا چاہیے۔

- **وفاقی حکومت کو دی گئی وسیع تر اختیارات کو کم کرنا:** دفعہ 35(2) کے تحت این سی پی ڈی پی کو وفاقی حکومت کے "انتظامی کنٹرول" میں رکھنے کی شرط رکھی گئی ہے۔ اس شق کو مسودے سے ہٹا دینا چاہیے تاکہ کمیشن کی خود مختاری اور اتھارٹی قائم رہ سکے۔ اس کے علاوہ، بل دفعہ 43(پالیسی ہدایات دینے کا اختیار) اور دفعہ 54(قوانین بنانے کا اختیار) کے ذریعے این سی پی ڈی پی کے کردار کو کمزور کرنے والی وسیع تر طاقتیں فراہم کرتا ہے، جو پاکستان میں ذاتی ڈیٹا کے تحفظ کے معاملات سے متعلق مختص اور آزاد ادارہ ہے۔

- **سرحد پار ڈیٹا کی منتقلی اور ڈیٹا لوکلائزیشن کے بارے میں موقف کا جائزہ:** دفعہ 32(سرحد پار منتقلی کے لیے حالات کے ڈھانچے) میں دی گئی دفعات کے حوالے سے، ڈیٹا لوکلائزیشن پر توجہ اس بات کو اجاگر نہیں کرتی کہ بڑے ڈیٹا فارمز کے لیے مناسب انفراسٹرکچر کی کمی ہے اوراس میں اس شق کو نافذ کرنے کے ممکنہ معاشی اخراجات کا بھی ذکر کیا گیا ہے جیسا کہ ایل آئی آر این ای ایشیا کی رپورٹ میں پاکستان میں ڈیٹا لوکلائزیشن پر کیا گیا ہے۔ رپورٹ کے مطابق، موجودہ بل کے نفاذ کے بعد اگلے سال میں16۔5 ارب ڈالر کا نقصان ہونے کی پیش گوئی کی گئی ہے اور اس کے ساتھ ساتھ بڑے پیمانے پر روزگار کے نقصانات بھی متوقع ہیں۔

ڈیٹا کسے کہتے ہیں؟

ڈیٹا سے مراد ہے معلومات، خاص طور پر وہ معلومات جو کہ اعداد و شمار پر منحصر ہو۔ ہمارے اپنے ڈیٹا کو ذاتی ڈیٹا یعنی پرسنل ڈیٹا کہا جاتا ہے اور اس کے اندر وسیع معلومات سمائی جا سکتی ہے۔ اس کا تذکرہ تفصیلی طور پر آگے کیا جائے گا۔

آج کے ڈیجیٹل دور میں ذاتی ڈیٹا کو اچھے معنوں میں ایک انتہائی قیمتی چیز[8] سمجھا جاتا ہے۔ یہ ہماری ذاتی زندگی کے بارے میں بہت سی معلومات فراہم کر سکتا ہے اور اگر اس کا غلط استعمال کیا جائے تو تشویش ناک خطرات لاحق ہو سکتے ہیں۔

ڈیٹا کا عام ہونا اس وقت اور خطرے کا باعث ہو سکتا ہے جب اس میں موجود معلومات ان لوگوں سے متعلق ہو جو کہ تاریخی طور پر حساس سمجھے جاتے ہیں جیسے کہ خواتین، بچے، مذہبی اور اقلیتی برادری۔
کسی بھی قسم کے ڈیٹا کا مالک ہونا، جو کہ حاصل کیا جاتا ہے، سنبھالا جاتا ہے یا پھر کسی بھی معنی میں استعمال کیا جاتا ہے آپ کو اس کی شناخت بنا دیتا ہے۔

> پرسنل ڈیٹا پروٹیکشن بل سیکشن s.2(j) کے تحت ڈیٹا سبجیکٹ سے مراد وہ شخص ہے جو کہ اس پرسنل ڈیٹا کا مالک ہو ۔

پرسنل ڈیٹا کسے کہتے ہیں؟

ذاتی ڈیٹا سے مراد وہ معلومات ہے جو کہ تمام لوگوں کو میسر نہ ہو اور جس کا تعلق کسی خاص شخص سے ہو۔ اس سے مراد وہ معلومات ہیں جس کی حفاظت انسانی پرائیویسی کے لیے ضروری ہے۔ ذاتی ڈیٹا میں بہت سے اقسام کے ڈیٹا کا شمار ہوتا ہے پرسنل پروٹیکشن بل 2023 میں شامل اقسام مندرجہ ذیل ہیں :

ذاتی ڈیٹا کا تحفظ بل ۲۰۲۳ کے تحت تعریف	ڈیٹا کی قسمیں
s.2(z) ذاتی ڈیٹا سے مراد وہ معلومات ہے کہ جس کا تعلق ڈیٹا کے مالک یعنی ڈیٹا سبجیکٹ سے ہو یا جس معلومات کے ذریعے اس کی مالک کی نشاندہی کی جا سکے ۔ذاتی حساس معلومات کا شمار بھی اس قسم کے ڈیٹا میں کیا جاتا ہے۔ البتہ جعلی نام یا بے نام موضوع پر منحصر معلومات کہ جس سے اس ڈیٹا کے مالک کی نشاندہی نہ کی جا سکے پرسنل ڈیٹا نہیں کہلاتا	ذاتی ڈیٹا
s.2(g) کریٹیکل پرسنل ڈیٹا سے مراد وہ معلومات ہے جو کہ کسی بھی انسانی خدمت پر معمور ملکی ادارے کے ملازمین کے پاس موجود ہو ۔اس میں وہ تمام معلومات بھی شامل ہیں جو کہ ادارے کی جانب سے حساس قرار دی جائے یا پھر جس میں کسی بھی قسم کے بین الاقوامی معاہدوں کے بارے میں خبر موجود ہو۔ البتہ ایسی معلومات جس کا عام عوام کو پتہ ہو اس کا شمار کریٹیکل پرسنل ڈیٹا میں نہیں کیا جاتا ۔	حساس ذاتی ڈیٹا (کریٹیکل پرسنل ڈیٹا)
s.2(a) اس سے مراد وہ ذاتی معلومات ہے کہ جس کو کچھ اس قسم کے تشکیلی مراحل سے گزارا جائے کہ جس کے بعد معلومات کا موضوع یعنی ڈیٹا سب جیکٹ کی نشاندہی ممکن نہ ہو سکے۔	انونی مائزڈ ڈیٹا
s.2(q) اس ڈیٹا سے مراد وہ معلومات ہے کہ جس میں کسی کی ذہنی اور جسمانی صحت کے متعلق تفصیلات موجود ہو ۔ ہسپتال کی ان تمام دستاویزات کا شمار بھی ہیلتھ ڈیٹا میں کیا جاتا ہے کہ جس میں کسی بھی شخص کے ماضی حال یا مستقبل کی صحت کے حالات کا تذکرہ ہو۔	صحت ڈیٹا ہیلتھ ڈیٹا

بائیو میٹرک ڈیٹا	s.2(c) بائیو میٹرک ڈیٹا وہ ذاتی معلومات ہے جو کہ کچھ مخصوص تکنیکی مراحل کے نتیجے سے بنتی ہے۔ان مراحل میں جسمانی اور رویوں پر مبنی عناصر شامل ہوتے ہیں۔یہ معلومات انسان کو ایک مخصوص شناخت دیتا ہے جیسے کہ چہرے کی شناخت اور انگلیوں کے نشانات۔
حساس ذاتی ڈیٹا	s.2(kk) اس میں مندرجہ ذیل ذاتی معلومات شامل ہے 1۔مالی معلومات جیسا کہ کریڈٹ کارڈ نمبر ،ڈیبٹ کارڈ نمبر یا پھر بینک اکاؤنٹ نمبر (سوائے شناختی کارڈ نمبر کے) 2۔ ذہنی صحت کے متعلق معلومات (صحت، جسمانی صحت ،نفسیاتی صحت اور طبی دستاویزات) 3۔شناختی کارڈ اور پاسپورٹ 4۔ جنسی معلومات 5۔مذہبی رجحان 6۔مجرمانہ دستاویزات 7۔سیاسی وابستگی 8۔بائو میٹرک معلومات 9۔ذات اور قبیلہ 10۔انفرادی نسل

ذاتی معلومات یعنی پرسنل ڈیٹا کی حفاظت ضروری ہے تاکہ شناختی اور شخصی چوری اور دھوکہ دہی سے بچا جا سکے ۔مزید یہ کہ اپنی ذاتی اور حساس معلومات تک کسی نامعلوم اور انجان شخص کو رسائی نہ پہنچائی جائے۔
اس لیے یہ جاننا ضروری ہے کہ پرسنل ڈیٹا ہوتا کیا ہے اور اس کی حفاظت آن لائن اور آف لائن کیسے کی جا سکتی ہے۔

پرائیویسی کیا ہے ؟

پرائیویسی ایسے تصور کو کہتے ہیں کہ جو کہ ایک انسان کو اجازت دیتا ہے کہ وہ اپنی ذاتی زندگی اپنے تک محدود رکھے۔

پرائیویسی انٹرنیشنل کے مطابق پرائیویسی اس بنیادی حق کا نام ہے کہ جس کے اوپر بہت سے انسانی حقوق کی بنیاد رکھی گئی ہے۔[9] اس وجہ سے پرائیویسی کو بہت اہمیت حاصل ہے۔ پرائیویسی رکھنے کا حق انسانی توقیر رکھنے کے حق سے جڑا ہوا ہے کیونکہ پرائیویسی کے بغیر انسانی توقیر قائم نہیں رہ سکتی۔

معلوماتی پرائیویسی بالخصوص اس حق کا نام ہے جو کہ انسان کو یہ اجازت دیتا ہے کہ اسے یہ اختیار حاصل ہو کہ کس طرح اس کی ذاتی معلومات کو جمع کیا جائے اور اس کا استعمال کیا جائے۔ یہ وہ بنیادی حق ہے جو کہ ہر شخص کو بغیر کسی رنگ، نسل، عمر، جنس اور کسی بھی شناخت کی تفریق کے بغیر حاصل ہے ۔ قانونی طور پر پاکستان کے باشندوں کو پرائیویسی کا حق آئین کے آرٹیکل 14 کے تحت تحت فراہم کیا جاتا ہے۔

بین الاقوامی سطح پر پرائیویسی کی تعریف کو دیکھا جائے تو آسٹریلین انفارمیشن کمشنر کے مطابق پرائیویسی کا حق[10] مندرجہ ذیل حقوق کا مجموعہ ہے :

- ا — کسی بھی قسم کی مداخلت سے آزادی
- ب — کسی کے ساتھ بھی آزادی سے منسلک ہونے کا حق
- پ — اس بات پہ اختیار ہونا کہ کون آپ کے متعلق معلومات کو دیکھ اور استعمال کر سکتا ہے

رضامندی کسے کہتے ہیں؟

کنسنٹ ایک ایسا تصور ہے کہ جس کی کوئی ایک جامع تعریف نہیں ہے اس کی تعریف وقت جگہ اور ملکی قانون کے مطابق بدلتی رہتی ہے۔ عمومی طور پر کنسنٹ کسی عمل، خیال ،ارادے پر رضا مندی کا نام ہے جو کہ کسی بھی شخص کے سامنے پیش کیا جاتا ہے۔

۱۸۷۲ قانونِ معاہدہ	۲۰۲۳ ذاتی ڈیٹا تحفظ بل
s.13 کنسنٹ کی تعریف: دو یا دو سے زیادہ افراد کی آپس میں رضامندی کو کہا جاتا ہے اگر وہ کسی بھی چیز پر ایک وقت میں ایک ہی معنوں میں رضامند ہوں۔	s.2(f) -"رضامندی" کا مطلب کوئی بھی آزادانہ طور پر دی گئی ، مخصوص ، اطلاع شدہ، اور غیر مبہم بات یا اشارہ جس کے ذریعے ڈیٹا سبجیکٹ اپنے ڈیٹا کی پراسیسنگ اور حصول کی اجازت دیتا ہے بشرطیکہ وہ کانٹریکٹ ایکٹ کی شق 13 اور 14 کے ساتھ موافق ہے۔

یہاں پر یہ سمجھنا انتہائی ضروری ہے کہ کنسنٹ یعنی رضامندی کو محض لفظی طور پر مفصل نہیں سمجھا جانا چاہیئے بلکہ رضامندی کا اظہار[11] آزادانہ طور پر کیا جاتا ہے۔ اس تمام صورتحال میں کسی بھی قسم کی دھوکہ دہی[12] کا عمل دخل نہیں ہوتا۔

سنِ بلوغت اور نابالغ پن کی عمر کیا ہے؟

مجورٹی بل[13] 1857 کے ترمیمی ایکٹ کے مطابق ہر وہ پاکستانی باشندہ جو اس ملک کا ڈومیسائل یا شہریت رکھتا ہے سنِ بلوغت کو 18 سال سے پہلے نہیں پہنچ سکتا۔

ابھی تک اس دفعہ میں کوئی تجدید نہیں کی گئی لہذا پاکستان میں بالغ کی حیثیت اٹھارہ سال کی عمر میں ہی حاصل کی جاتی ہے جبکہ 17 سال یا اس کم عمر شخص نا بالغ ہی تصور کیا جاتا ہے۔

نابالغان کے لیے خصوصی اقدامات

بہت سے سوشل میڈیا پلیٹ فارمز[14] نے نا بالغوں کیلئے خصوصی اقدامات متعارف کروائے ہیں۔ جو کہ مندرجہ ذیل ہیں:

ایپ، پلیٹ فارم یا ویب سائٹ	اقدامات
میٹا (فیس بک، انسٹا گرام، واٹس ایپ):	میٹا کے پاس کم عمر نوجوانوں کے لیے ایپ کے حساب سے ذرا مختلف حفاظتی قواعد و ضوابط ہیں: 1۔ سولہ سال سے کم عمرلوگوں کیلئے فیس بک پر مزید پرائیویٹ سیٹنگز کا حصول موجود نہیں۔ 2۔ اے آئی کے ذریعے عمر کی جانچ پڑتال تاکہ عمر کے مطابق تجربات سے روشناس کیا جائے۔ 3۔ محدود اشتہاراتی ہدف بندی اور وہ تھوڑی دیر کے لیے ایپس کو بند کرنے کے لیے خاموش موڈ استعمال کر سکتے ہیں۔
ٹویٹر ۔ایکس:	ٹویٹر استعمال کرنے کے لئے کم از کم تیرہ سال کا ہونا ضروری ہے ۔ کچھ ممالک میں والدین یا سرپرست کو اپنے بچوں کی جانب سے رضامندی ظاہر کرنی پڑتی ہے کہ وہ ان کے پرسنل ڈیٹا تک رسائی حاصل کر سکیں اور اسے استعمال کر سکیں۔
سنیپ چیٹ:	سنیپ چیٹ نے ایک ان ایپ ٹول متعارف کرایا ہے جس کو فیملی سینٹر کہا جاتا ہے۔ اس کے مطابق والدین سرپرست یا پھر کچھ عزیز واقارب جو کہ پچیس سال سے بڑے ہوں وہ اپنے تیرہ سے اٹھارہ سال کے بچوں کے ساتھ اس فیملی سینٹر کا حصہ بن سکتے ہیں اور ان کی طرف سے کی گئی گفتگو کے کسی خاص مواد کو ظاہر کیے بغیراس چیز پر نظر رکھ سکتے ہیں کہ پچھلے سات دنوں میں ان کے بچے نے کس کے ساتھ روابط رکھے ہیں۔

ٹک ٹاک:	ٹک ٹاک کے اکاؤنٹ تک رسائی حاصل کرنے کے لیے عمر کا تیرہ سے پندرہ سال ہونا ضروری ہے اور ان کے اکاؤنٹ نجی نوعیت کے بنتے ہیں۔ جبکہ پیغامات کے تبادلے کے لیے عمر کا سولہ سال یا اس سے بڑا ہونا ضروری ہے۔
پِن ٹرسٹ:	16 سال سے کم عمر کے نوعمر اکاؤنٹس اب بائی ڈیفالٹ نجی ہیں اور عمر کی تصدیق ان کی پالیسیوں کا حصہ ہے۔
یو ٹیوب:	اس میں بچوں کے اکاؤنٹ کے متعلق دو اختیارات دیے گئے ہیں؛ ایک والدین کی سرپرستی میں بچوں کا اکاؤنٹ اور دوسرا یوٹیوب کڈ ایپ۔ اس ایپ میں والدین یہ اختیار رکھتے ہیں کہ اپنے بچوں کو کس قسم کی چیزیں دکھانی ہیں، مزید یہ کہ ان کو یہ بھی اختیار حاصل ہوتا ہے کہ وہ کتنی دیر تک اپنے بچوں کو یوٹیوب دکھا سکتے ہیں۔
ٹیک اٹ ڈاؤن:	عالمی ادارہ برائے گمشدہ اور زیادتی شدہ بچوں نے یہ ایک ٹول متعارف کرایا ہے ۔ (https://takeitdown.ncmec.org/)جس کے ذریعے بچوں یا پھر نوجوانوں کی نجی تصاویر کے ساتھ کی جانے والی زیادتی کا سد باب کیا جاتا ہے۔ یہ ٹول نا مناسب عریاں یا جنسی تصویروں اور ویڈیو کا ایک بے ترتیب خاکہ سا بنا دیتا ہے جو کہ پھر مزید سوشل میڈیا ویب سائٹ پر نہیں پھیلایا جاتا ۔

نجی اور عوامی آن لائن مقامات میں فرق

عوامی مقامات پر کسی بھی شخص کی بات چیت اور حرکات تک رسائی ہر شخص کو ہو سکتی ہے جیسا کہ عوامی ویب سائٹس سوشل میڈیا اکاؤنٹس۔ ان جگہوں پر شائع کی جانے والی معلومات تک تمام عوام کو رسائی حاصل ہوتی ہے مزید یہ کہ یہاں پر پرائیویسی کا معیار کسی بھی نجی ویب سائٹ کے پرائیویسی کے معیار سے مختلف ہوتا ہے۔[15]

تاہم، نجی جگہ میں وہ علاقے شامل ہیں جہاں افراد اپنی ذاتی، خفیہ سرگرمیاں کرتے ہیں، جیسے کہ نجی ای میلز، خفیہ پیغامات، اور محفوظ آلات پر محفوظ کردہ ذاتی ڈیٹا۔[16]

ڈیٹا پروسیسر اور ڈیٹا کنٹرولرز کون ہوتے ہیں؟

ڈیجیٹل ذرائع کے تحت ڈیٹا بہت طریقوں سے اکٹھا ترتیب اور محفوظ کیا جاتا ہے۔ مثال کے طور پہ جب کوئی صارف کسی ویب سائٹ پر جاتا ہے توبراؤزنگ ڈیٹا اس حوالے سے جمع کیا جاتا ہے کہ صارف نے کیا ملاحظہ کیا، وہاں کتنا وقت گزارا اور کس چیز پر کلک کیا ۔ کوئی بھی شخص جو اپنا مطلوبہ ڈیٹا اکٹھا کرتا ہے، محفوظ کرتا ہے اور اسے پرکھتا ہے وہ ڈیٹا کلیکٹر کہلاتا ہے۔

یہ جاننا ضروری ہے کہ ڈیٹا اکٹھا کرنے والے حکومت، نجی سوشل میڈیا کمپنیاں جیسے فیس بک یا ٹویٹر وغیرہ کے ساتھ ساتھ کوئی بھی کمپنیاں ہو سکتی ہیں جنہیں خدمات فراہم کرنے کے لیے ذاتی ڈیٹا کی ضرورت ہوتی ہے۔ یہ ڈیٹا اکٹھا کرنے والے ہیں جو رضامندی کے ذریعے قانونی ذرائع سے ڈیٹا اکٹھا کرتے ہیں۔ لیکن کچھ لوگ ڈیٹا اکٹھا کرنے کے لیے غیر قانونی ذرائع، جیسے ہیک یا ڈیٹا لیک کا استعمال کرتے ہیں۔

ڈیٹا ہولڈرز وہ افراد اور ادارے ہوتے ہیں جو کہ اپنے صارفین کا ڈیٹا محفوظ کر کے رکھتے ہیں۔ یہ وہ ڈیٹا بھی سنبھال کر رکھتے ہیں جو صارفین انہیں مہیا کرتے ہیں۔ ڈیٹا ہولڈر ڈیٹا کلیکٹر بھی ہو سکتے ہیں ۔جبکہ کوئی اور شخص یا ادارہ جس کو ڈیٹا کلیکٹرز ڈیٹا فراہم کرتے ہیں وہ بھی ڈیٹا ہولڈرز کہلائے جا سکتے ہیں۔

ڈیٹا پروٹیکشن بل دونوں ڈیٹا کلیکٹر اور ڈیٹا ہولڈرز کو ڈیٹا کے ساتھ منسلک کرتا ہے۔

s.2(h) ڈیٹا کنٹرولر سے مراد وہ شخص،ادارہ یا گورنمنٹ ہے جو کہ اکیلے یا مل کر یہ اختیار رکھتے ہوں کہ ڈیٹا کے اجماع اس کے استعمال اور اس کے عام کرنے کا فیصلہ کر سکیں۔

s.2(i) ڈیٹا پروسیسر سے مراد وہ شخص، ادارہ یا گورنمنٹ ہے جو اکیلے یا پھر اور لوگوں کی مدد سے ڈیٹا کنٹرولر کی ذمہ داری پر ڈیٹا کو ترتیب اور تشکیل کے مراحل سے گزارے۔

ڈیٹا کا تحفظ کیوں ضروری ہے؟

تکنیکی ترقی کے نتیجے میں ڈیجیٹل دنیا میں زیادہ ترقی ہوتی ہے۔ تاہم، اس کا مطلب یہ بھی ہے کہ ٹیکنالوجی تیزی سے خطرے کا سامان بننے کی صلاحیت رکھتی ہے۔

نجی معلومات کا ہونا ضروری ہے کیونکہ اس سے کسی بھی شخص کو یہ اختیار حاصل ہوتا ہے کہ وہ اپنے ڈیٹا کی حفاظت کر سکے ۔ بڑھتی ہوئی ٹیکنالوجی کا خطرہ ڈیٹا کے غلط استعمال کی شکل اختیار کرتا جا رہا ہے لہذا یہ ضروری ہے کہ ڈیٹا کو محفوظ رکھا جائے۔ ماضی قریب میں نادرہ، ایف آئی اے[17]، دارالامان راولپنڈی[18] اور سیف سٹی پروجیکٹ[19] جیسی مثالیں موجود ہیں جن میں حساس ڈیٹا تک رسائی حاصل کر کے اس کا غلط استعمال کیا گیا ہے۔ ان واقعات نے ملک کے باشندوں کو بہت سے طریقوں سے باور کروایا ہے کہ کس طرح سے ڈیٹا تک رسائی حاصل کی جا سکتی ہے

بین الاقوامی سطح پر کیمبرج انیلیٹیکا ڈیٹا سکینڈل یہ واضح کرتا ہے کہ کس طریقے سے ڈیٹا کا غلط استعمال جمہوری عمل کو متاثر کر سکتا ہے۔ایک صحافی کی خبر[20] نے اس بات کی نشاندہی کی کہ کس طرح سے غلط طریقے سے استعمال کیا جانے والا ڈیٹا جو کہ لوگوں کی فیس بک پروفائل سے حاصل کیا گیا تھا اس سے لاکھوں کے حساب سے ووٹر پروفائل بنائی گئی اور صدارتی انتخابات کو متاثر کرنے کی کوشش کی گئی۔[21]

ٹیکنالوجی اب ہماری زندگیوں کا لازمی جزو بنتی جا رہی ہے ۔ ہماری ذاتی معلومات، ہمارا ڈیٹا اب مختلف قسم کے آلات میں جمع ہوتا ہے۔ لہذا ضرورت اس امر کی ہے کہ ڈیٹا کی حفاظت کے لیے اقدام اٹھائے جائیں۔ افراد اور کمپنیاں چاہے وہ نجی ہوں یا پھر گورنمنٹ کی انہیں چاہیے کہ ڈیٹا کی حفاظت کو لازمی قرار دیں۔

ڈیٹا خود مختاری

خود مختاری کا تصور ہمارے آئین سے جڑا ہوا ہے جو کہ ہر شخص کو جسمانی آزادی اور توقیر کا حق دیتا ہے۔ یہ بنیادی حق یہ باور کرواتا ہے کہ ہر شخص کو اپنے جسم پر مکمل اختیار حاصل ہے اور وہ کسی کے بھی بے جا عمل دخل سے آزاد ہے۔ اسی طرح کسی شخص کا اپنے ڈیٹا کے اوپر اختیار رکھنا بھی آئین میں شامل حقیقی پرائیویسی کی ایک تصویر ہے۔ یہ لوگوں کو یہ یقین دلاتا ہے کہ ان کا اپنے ڈیٹا کے اوپر اسی طرح اختیار ہے جس طرح کہ ان کو اپنے جسم پر ہے ۔یہ قانون محمد رحمت اللہ بمقابلہ ریاست[22] والے معاملے میں سمجھا جا سکتا ہے کہ جہاں پر ڈیٹا کا آزادانہ حیثیت ہونا ایک بنیادی حق سمجھا جاتا ہے۔ یہ بنیادی حق ہر شخص کو اس قابل کرتا ہے کہ وہ اپنے ڈیجیٹل فٹ پرنٹ پر اختیار رکھیں اور اپنی ذاتی معلومات کے استعمال کے متعلق فیصلے کر سکے۔

تکنیک کی بنیاد پر صنفی تشدد و زیادتی (TF-GBV)

پرائیویسی کے خلاف ورزی نے صنفی حدود بھی پار کر لی ہیں۔

جیسا کہ ڈی آر ایف کے جاری کردہ وائٹ پیپر میں: جنوب اور جنوب مشرقی ایشیا کے تناظر[23] میں لوگوں پہ براہِ راست ان کی جنس کی بنیاد پر ہونے والے ریاستی ، صنفی بنیاد پر تشدد جیسے اقدامات کئے گئے۔ بعض افراد کو صرف اپنی جنس کی بدولت بے جا خطرات کا سامنا ہوتا ہے۔

یہ ٹیک فیسلٹیٹڈ جینڈر بیسڈ وائلنس ٹی ایف جی بی وی کی تعریف کچھ اس طرح کرتا ہے کہ یہ انٹرنیٹ اور مختلف ڈیجیٹل پلیٹ فارمز کے استعمال سے خواتین اور صنفی اور جنسی اقلیتی برادری کے ارکان پر خوف اور دہشت گردی بڑھانا ہے۔

مارچ 2020 میں اقوامِ متحدہ کے ایک اہم رپورٹر جوزف کینٹاکی نے صنفی برابری کے متعلق کہا کہ یہ دنیا بھر میں پرائیویسی کو عمل میں لانے سے حاصل ہوتی ہے۔

اس کی رپورٹ کا ایک اقتباس یہ کہتا ہے:

> صنفی پرائیویسی کی بے حرمتی کے نتیجے میں بہت سے خطرات نے جنم لیا ہے۔ اس کے نتیجے میں خطرناک قسم کی دہشت گردی اور یہاں تک کہ اموات بھی پیش آئی ہیں۔[24]

مزید یہ کہ ڈیٹا کا غلط استعمال کا شکار زیادہ تر صرف وہ ہوتے ہیں جن کو معاشرے میں نظر انداز کیا جاتا ہے لہذا ایسی صورتحال میں پرائیویسی کی حفاظت کرنا ایک انتہائی ضروری عمل ہے۔

پرائیویسی پر پاکستانی فقہ

محترمہ بے نظیر بھٹو بمقابلہ صدرِ پاکستان
(PLD 1998 Supreme Court 388)

خلاصہ: اس عہد ساز مقدمہ میں پاکستان کی سپریم کورٹ نے آئین کے آرٹیکل 14 کے تحت ٹیلی فون کالز کی ریکارڈنگ اور بنا اجازت سنوائی جیسی قانونی پیچیدگیوں کو پرکھا۔ اس مقدمے میں رائج الوقت وزیر اعظم پاکستان، بے نظیر بھٹو کی حکومت پر الزامات لگائے گئے تھے کہ ان کی حکومت غیر قانونی طور پر متعدد ججز، سیاسی رہنماؤں اور فوجی افسران کے ٹیلی فون ٹیپ کرنے میں ملوث ہے۔ عدالت نے یہ حکم صادر کیا کہ ایسے غیر قانونی اقدامات سے ایک شخص یا ادارے کے وقار اور حق رازداری کو بری طرح مجروح کیا گیا ہے، اور اس طرح پبلک یعنی عوامی جگہوں کو بھی رازداری کے دائرہ کار میں شامل کر لیا گیا۔

متعلقہ اقتباس: پرائیویسی کی خلاف ورزی کا انسانی وقار سے باضابطہ طور پر تعلق ہے۔ اگر کوئی شخص اپنی توقیر کی سلامتی چاہتا ہے یا اپنی زندگی عزت اور شان سے گزارنا چاہتا ہے تو ضروری ہے کہ اس کی پرائیویسی چاہے وہ گھر پر موجود ہو یا باہر، اس کی حفاظت کی جائے اور اسے غیر قانونی عمل دخل سے بچایا جائے۔ آرٹیکل 14 کے تحت جس حق کا ذکر کیا گیا ہے وہ فرد واحد کو کسی مخصوص جگہ تک محدود نہیں کرتا بلکہ ہر اس مقام پر لاگو ہوتا ہے جہاں وہ شخص موجود ہو۔ (پیراگراف 30)

منظور احمد بمقابلہ ریاست
(1990 MLD 1488)

خلاصہ: آئینِ پاکستان کے آرٹیکل 14 کے مطابق کسی کی پرائیویسی میں غیر قانونی طور پر دخل جیسے کہ ریکارڈنگ کرنا، کان لگا کر بات سننا، بنا اجازت سنوائی، اور گھر کے اندر تصویریں کھینچنا سختی سے منع ہے اور اسلام میں بھی ان تمام حرکات کی اجازت نہیں ہے۔

متعلقہ اقتباس: آئین کے آرٹیکل 14 کے تناظر میں کان لگا کر بات سننا ریکارڈنگ کرنا یا کسی کے گھر کے اندر تصویریں کھینچنا یہ سب عوامل کسی کی پرائیویسی میں مداخلت کے زمرے میں آتے ہیں اور اس کی اجازت نہ تو آئین میں ہے اور نہ ہی اسلام میں۔ (پیراگراف 5)

محمد نواز بمقابلہ ایڈیشنل ڈسٹرکٹ اور سیشن جج
(سپریم کورٹ P L D 2023 461)

خلاصہ : غیر قانونی طور پر ڈی این اے اکٹھا کرنا پرائیویسی، خود مختاری ، اور آزادی کے حقوق کی خلاف ورزی کرتا ہے۔

ذاتی معلومات میں بیرونی مداخلت سے تحفظ کو بھی اسی کیس میں زیر بحث لایا گیا۔
آئین کے آرٹیکل 14 نے پرائیویسی کو بنیادی انسانی حق قرار دیا ہے جس کے ذریعے انسان کے ذاتی انتخابات اور رہن سہن کو گھر کی چار دیواری سے آگے بڑھ کر حفاظت دی گئی ہے۔ پرائیویسی انسان کی عزت و توقیر اور شخصی پہچان کے لیے نہایت ضروری ہے۔

پرائیویسی کے حق میں کسی بھی شخص اور اس کی ذاتی زندگی کو بیرونی مداخلت سے محفوظ کرنا شامل ہے۔ یہ حق ہر انسان کی ذاتی معلومات، بات چیت کو ناجائز مداخلت سے بچاتا ہے خواہ وہ مداخلت گورنمنٹ کی جانب سے ہو یا پھر کسی ادارے یا شخص کی جانب سے ہو۔ پرائیویسی قائم رکھنا شخصی آزادی کے لیے بہت ضروری ہے ۔اس سے انسان اس قابل ہوتا ہے کہ بغیر کسی قسم کی نگرانی کے خوف اور ڈر سے اپنی مرضی کے مطابق کوئی بھی عمل کر سکے۔ اس طرح اس کی ذاتی معلومات بھی کسی پر افشا نہیں ہوتی۔ (پیراگراف 6)

ڈیٹا مالکان کے حقوق

ڈیٹا پروٹیکشن بِل 2023 کے مسودے کے مطابق ڈیٹا مالک کے کلیدی حقوق میں شامل ہیں۔

رسائی کا حق PDPB 2023 s.16 کے تحت ڈیٹا کا مالک یہ اختیار رکھتا ہے کہ وہ جان سکے کہ اس کے ڈیٹا کنٹرولر نے اس سے متعلق ڈیٹا ترتیب دے دیا ہے یا کہ ابھی تک اس کا ڈیٹا ترتیبی اور تکمیلی مراحل سے گزر رہا ہے۔ ڈیٹا سبجیکٹ اپنے ڈیٹا کنٹرولر کو ایک تحریری درخواست بھی لکھ سکتا ہے، ایک مقررہ فیس کی ادائیگی پر، کہ اس کو ڈیٹا کے ترتیبی مراحل تک رسائی دی جائے نیز یہ کہ وہ اپنے ڈیٹا کی ایک کاپی بھی مانگ سکتا ہے۔

درستگی کا حق PDPB 2023 s.19 کے تحت یہ وہ حق ہے کہ جس میں ڈیٹا سبجیکٹ یا مالک کو یہ اختیار حاصل ہوتا ہے کہ اگر اس کا ڈیٹا نامکمل غلط یا کسی بھی لحاظ سے گمراہ کن ہے تو وہ ڈیٹا کنٹرولر کو یہ درخواست کر سکتا ہے کہ اس کے ڈیٹا میں درستگی کی جائے۔

ڈیٹا کو حذف کرنے کا حق PDPB 2023 s.26 کے تحت یہ وہ حق ہے کہ جس میں ڈیٹا سبجیکٹ کو یہ اختیار حاصل ہو کہ وہ ڈیٹا کنٹرولر سے درخواست کر سکے کہ اس کا ذاتی ڈیٹا حذف کر دیا جائے ڈیٹا کنٹرولر 14 دنوں میں ڈیٹا حذف کرنے کا مجاز ہوتا ہے اگر :

۔ذاتی ڈیٹا جس مقصد کے لیے حاصل کیا گیا ہو وہ اس کام کے لیے اہم نہ رہے
۔ ڈیٹا مالک ایسی رضامندی سے دستبردار ہوجائے جس پر طریقِ کار کا اطلاق سیکشن 23 (رضامندی کے حق سے دستبرداری) کے سب سیکشن (1) ہوتا ہواور جس طریقِ کار میں اور کوئی قانونی حقائق نہ ہوں؛ یا
۔ ڈیٹا مالک سیکشن 23 کے سب سیکشن (2) کے تحت ڈیٹا کی ترتیب و تشکیل پر اعتراض اٹھائے
۔ڈیٹا غیر قانونی طریقے سے تشکیل ہو؛ یا
۔ قانونی تقاضوں کو پورا کرنے کے لیے ڈیٹا کو ختم کرنا ضروری ہو

انتخاب کا حق PDPB 2023،s.27 کے تحت ڈیٹا سبجیکٹ کو یہ حق حاصل ہے کہ وہ کسی بھی شخص کا انتخاب کر سکتا ہے جو کہ اس کی جگہ اس کے ڈیٹا کے معاملات کی نگرانی کرے، موت یا معذوری کی صورت میں۔

ڈیٹا کی از سر نو ترتیب اور اس کے متعلق شکایت کا حق PDPB 2023،s.28 کے تحت یہ حق ڈیٹا مالک کو یہ اختیار دیتا ہے کہ وہ کسی بھی قسم کی شکایت کی صورت میں ڈیٹا کنٹرولر کو تحریری درخواست لکھ سکتا ہے۔ ڈیٹا کنٹرولر پر یہ لازم ہے کہ وہ جلد از جلد شکایت کے سد باب کے حوالے سے کام کرے۔ اگر ڈیٹا کنٹرولر ڈیٹا مالک کی شکایت کو دور نہ کر سکے یا پھر اس کی درخواست کا جواب نہ دیں تو ڈیٹا مالک کو یہ حق حاصل ہے کہ وہ اپنی شکایت نیشنل کمیشن برائے ذاتی ڈیٹا پروٹیکشن (این-سی-پی ڈی-پی) کو درج کروائے۔

ڈیٹا کی منتقلی اور خود کار تشکیل PDPB 2023،s.29 کے تحت یہ وہ حق ہے کہ جس میں ڈیٹا مالک اپنا ذاتی ڈیٹا، ڈیٹا کنٹرولر سے حاصل کر سکتا ہے۔ یہ ڈیٹا بے ترتیب اور بے ہنگم نہیں ہونا چاہیے اور یہ اس قابل ہو کہ کسی مشینی طور پر پڑھا جا سکے۔ ڈیٹا مالک کو یہ اختیار حاصل ہو گا کہ وہ اپنا ذاتی ڈیٹا کسی اور ڈیٹا کنٹرولر یا پروسیسر کو بغیر کسی اعتراض کے فراہم کر دے، جہاں:

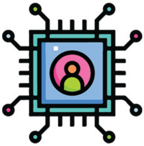
ا۔ ڈیٹا مالک نے اپنا مکمل کنسنٹ دیا ہو۔
ب۔ ڈیٹا کا اجرا خودکار طور پر پروسیس کیا جا رہا ہو۔

یہ شق اس استثناء کے ساتھ لاگو ہے کہ ڈیٹا کی پروسیسنگ مفاد عامہ کے مقصد کی لئے کی جا رہی ہواس کے علاوہ ڈیٹا مالک کو یہ حق حاصل ہو گا کہ وہ محض خودکار پروسیسنگ کے بلبوتے پر کیے جانے والے فیصلوں پر اکتفا نہ کرے جیسا کہ پروفائلنگ، جس سے کہ قانونی ذمہ داری عائد ہوتی ہو یہ جس سے ڈیٹا مالک کو بہت خطرہ پہنچا سکتا ہے ماسوائے تب کہ اگر ڈیٹا مالک نے رضامندی کا اظہار کیا ہو۔

مزید یہ کہ ڈیٹا سبجیکٹ کو یہ حق حاصل ہے کہ وہ ڈیٹا کنٹرولر سے مندرجہ ذیل چیزوں کا تقاضہ کر سکے:

۔خود کار طریقوں کے متعلق مخصوص معلومات جس میں پروفائلنگ بھی شامل ہے ۔
۔ انسانی مداخلت۔

ڈیجیٹل شناخت کے مضمرات



کچھ لوگوں کو یہ غلط فہمی ہوتی ہے کہ اگر وہ اپنے سوشل میڈیا سے مواد کو ہٹا دیں تو وہ ہمیشہ کے لیے ختم ہو جاتا ہے۔ حالانکہ ایسا نہیں ہے اگر کوئی ویب سائٹ یا مواد ختم ہو بھی جاتا ہے تو وہ پھر بھی کسی نہ کسی صورت میں آن لائن کیچ اکثر ان اندراجات کو برقرار رکھتے ہیں، مطلب یہ ہے کہ آن لائن اشتراک کردہ کوئی بھی چیز واقعی نجی نہیں ہے۔

کوکیز[27]	کیشے[26]	میٹا ڈیٹا[25]
کوکیز ڈیٹا کہ وہ چھوٹے حصے ہیں جو کہ صارفین کے ویب براوزر کے ذریعے ان کے کمپیوٹر میں محفوظ ہو جاتے ہیں۔ یہ کچھ اس طرح سے مرتب کیے گئے ہیں کہ ویب سائٹ اپنے پاس معلومات کو محفوظ رکھ سکے۔ اس سے صارفین کی براوزر پر کی جانے والی نقل و حرکت بھی محفوظ ہو جاتی ہے۔	کیچ ایک ایسے ہارڈویئر اور سافٹ ویئر کا حصہ ہے جو کہ مستقبل میں کی جانے والی ڈیٹا کی طلب کو پورا کرتا ہے۔ کیچ میں موجود ڈیٹا پہلے کیے جانے والے کسی کام کا نتیجہ ہوتا ہے یا پھر ڈیٹا کی ایک کاپی کہیں اور محفوظ ہوئی ہوتی ہے۔	میٹا ڈیٹا ایک ایسا ڈیٹا ہوتا ہے جو کہ دوسرے ڈیٹا کے متعلق معلومات فراہم کرتا ہے جیسا کہ مصنف کا نام، شائع ہونے کی تاریخ، مرتب ہونے کی تاریخ اور بہت کچھ ۔ یعنی کہ یہ ڈیٹا کسی بھی ڈیٹا کو سمجھنے، ترتیب دینے اور اس کو تلاش کرنے میں مدد دیتا ہے۔

ضروری ہے کہ لوگ انٹرنیٹ پر اپنے بارے میں کوئی بھی معلومات ڈالتے ہوئے احتیاط برتیں۔ اس کے علاوہ یہ بھی ایک اچھا طریقہ ہے کہ باقاعدگی سے اپنا نام سرچ انجن پر تلاش کیا جائے اور دیکھا جائے کہ آپ کے بارے میں کوئی غلط معلومات تو نہیں موجود جو آپ کی مرضی کے خلاف ڈال دی گئی ہوں۔ آن لائن کیا جانے والا ہر کام اپنے پیچھے ایک ڈیجیٹل[28] ثبوت چھوڑ دیتا ہے۔ یہ ثبوت مختلف ویب سائٹ کی جانب سے حاصل کر لیا جاتا ہے اس کی نشاندہی کی جاتی ہے اور اکثر کسی مشتہر کو بیچ دیا جاتا ہے۔ مختلف سوشل میڈیا کے ذرائع جیسے کے میٹا اور بہت سی مفت آن لائن ایپلیکیشن آپ کے موبائل تک رسائی حاصل کرتی ہیں اور ڈیٹا جمع کرتی ہیں۔ ضروری ہے کہ کسی بھی ایپلیکیشن کی اجازت نامے کو غور سے پڑھا اور سمجھا جائے۔

بڑھتی ہوئی ڈیجیٹائزیشن اور اس کے پرائیویسی پر اثرات

پاکستان میں بڑھتے ہوئے ڈیجی ٹائزیشن کے بہاؤ نے روزانہ کی بات چیت، کاروبار کے طور طریقے اور روزمرہ کی طرز زندگی کو کافی حد تک بدل ڈالا ہے۔ لیکن اس بڑھتے ہوئے عمل نے پرائیویسی اور ڈیٹا کی حفاظت پر سوال اٹھائے ہیں۔ ذاتی معلومات کی آسانی سے رسائی سائبر کرائم اور ڈیٹا کے چوری ہونے جیسے عوامل کو ہوا دیتی ہے۔ یہ چوری کیا ہوا ڈیٹا اکثر ڈارک ویب پر بیچ[29] دیا جاتا ہے۔اسی طرح مختلف ویب سائٹ پر ایک ہی پاس ورڈ کا استعمال بھی سائبر حملوں کا باعث بنتا ہے۔ جس کے نتیجے میں بہت سے مالی اور شناختی نقصانات کا سامنا کرنا پڑتا ہے۔ ذاتی معلومات کی حفاظت کے لیے ضروری ہے کہ صارفین باقاعدگی سے اپنا پاس ورڈ تبدیل کریں، اپنی آن لائن موجودگی کا خیال رکھیں اور آن لائن کوئی بھی چیز انتہائی احتیاط سے ڈالیں۔

اصطلاح	تعریف	پی ڈی پی بی کی تعریف	خصوصیات
ڈیٹا بریچ [30]	یہ ایک ایسا واقعہ ہے کہ جہاں پر کوئی شخص غیر قانونی طریقے سے آپ کے ذاتی، محفوظ کیے گئے اور حساس ڈیٹا تک رسائی حاصل کر سکتا ہے۔ یہ واقعہ سائبر حملوں ہیکنگ اور ڈیٹا چوری کے نتیجے سے پیش آتا ہے	s.2(a,a) پرسنل ڈیٹا بریچ سے مراد حفاظتی اقدامات کے خلاف ورزی ہے جو کہ غیر قانونی تباہی کا باعث بنتی ہے۔ اس کے علاوہ اس کے ذریعے ذاتی معلومات یا ڈیٹا جو کہ محفوظ کیا گیا ہوتا ہے ترتیب دیا جا رہا ہوتا ہے۔ یہ گم ہو سکتا ہے، اس کے ساتھ چھیڑ چھاڑ کی جا سکتی ہے اور اس تک رسائی بھی حاصل کی جا سکتی ہے۔	یہ جان بوجھ کر کیے جانے والے نفرت آمیز عوامل پر مبنی ہے جس میں ڈیٹا تک غیر قانونی طور پر رسائی حاصل کی جا سکتی ہے. اس میں زیادہ تر سائبر حملوں اور ہیکنگ کو آلہ کار بنایا جاتا ہے
ڈیٹا لیک [31]	ڈیٹا لیک اس صورت کو کہتے ہیں کہ جب نا دانستہ طور پر ڈیٹا عوام تک پہنچ جائے۔ یہ زیادہ تر اندرونی غلطیوں غلط استعمال یا پھر غیر ذمہ داری کی وجہ سے ہوتی ہے-	مسودہ میں اس کی کوئی تعریف موجود نہیں ہے۔	زیادہ تر غیر دانستہ طور پر ہوتی ہے۔ ذاتی غلطی یا پھر غیر ذمہ داری کی وجہ سے حساس معلومات لوگوں کے سامنے آجاتی ہے

حاصل کلام

پرائیویسی کے حق کو مختلف بین الاقوامی معاہدوں اور ملکی اور صوبائی منشور کے تحت تمام افراد کے لیے ایک بنیادی حق قرار دیا گیا ہے۔ پاکستان ایک جمہوری مملکت ہے جہاں ہر فرد کو بنیادی حقوق ملنے چاہئیں۔ ٹیکنالوجی کی بڑھتی ہوئی ترقی سے ڈیٹا کے استعمال کا ایک طوفان آیا ہے اور ڈیٹا کی حفاظت کا ایک شفاف نظام نہ ہونے کی وجہ سے ملکی باشندوں کو مشکلات کا سامنا ہے۔ پاکستان کی عدلیہ جو کہ کسی بھی ریاست کا ایک لازمی اور اہم جزو ہوتی ہے اس کی یہ ذمہ داری ہے کہ ذاتی ڈیٹا کے متعلق لوگوں کے مسائل کا سدباب کرے۔ اس کے علاوہ کچھ اس طرح کے مثالی اقدام اٹھائے جائیں جو کہ انسانی عزت و توقیر اور پرائیویسی کی حقوق کی فراہمی کر سکیں۔

پاکستان میں پالیسی سازوں کا شہریوں کے حقوق کے تحفظ میں اہم کردار ہے، خاص طور پر جب ڈیجیٹل خطرات بڑھ رہے ہوں۔ ذاتی ڈیٹا کی کمزوریاں، غیر متوازن طریقے اور نگرانی کی کمی اب سنگین مسائل بن چکے ہیں، اس لیے ضروری ہے کہ ایک مکمل قانون سازی متعارف کرائی جائے جو پرائیویسی کے حق اور انسانی عزت کی حفاظت کرے۔ ڈیٹا کے استعمال کو باقاعدہ بنانے اور جوابدہی کو یقینی بنانے کے لیے عملی اقدامات اٹھا کر، پالیسی ساز شہریوں کے ڈیجیٹل حقوق کا تحفظ کرنے اور ڈیٹا پرائیویسی کے حوالے سے قانونی ڈھانچے میں اعتماد پیدا کرنے کے لیے مضبوط مثال قائم کر سکتے ہیں۔