Majallah-e-Talim o Tahqiq **مجلہ تعلیم وتحقیق**
Markaz Talim o Tahqiq, Gulshan-e-Taleem, Sector H-15, Islamabad, Pakistan
مرکز تعلیم و تحقیق، گلشنِ تعلیم، ایچ۔۱۵، اسلام آباد، پاکستان
ISSN (P): 2618-1355, ISSN (Online): 2618-1363
Issue 3, Vol ,8 , July–September ,2026 شمارہ ۳، جلد ۸، جولائی–ستمبر، ۲۰۲۶

ڈیجیٹل شواھد: شریعت اور پاکستانی قانون کے تناظر میں ایک تجزیاتی مطالعہ

Digital Evidence: An Analytical Study in the Light of Shariah and Pakistani Law

Suleman[1]
Wasi Ur Rehman[2]

Abstract

Digital evidence has become an essential component of modern judicial proceedings due to the rapid advancement of information technology. This study analytically examines the nature, evidentiary status, and legal and Sharīʿah implications of digital evidence in the light of Islamic principles and Pakistani law. Particular attention is given to its classification as *kitābah* (written evidence), *iqrār* (admission), testimony, and *qarā'in* (circumstantial evidence), as well as its treatment under the *Qanun-e-Shahadat Order, 1984*, particularly Articles 73 and 164. The study also examines the requirements of authentication, integrity, reliability, preservation, and chain of custody. It concludes that the digital nature of evidence does not by itself determine its evidentiary status; rather, its legal and Sharīʿah value depends upon its source, attribution, authenticity, relevance, reliability, and the applicable standards of proof. The study highlights both the areas of compatibility and the differences between Sharīʿah principles and Pakistani law regarding the use and evidentiary weight of digital evidence.

Keywords: Digital Evidence, Sharīʿah, Pakistani Law, Qanun-e-Shahadat Order, Electronic Evidence, *Qarā'in*, Authentication.

[1] PhD Scholar, International Islamic University Islamabad (IIUI), sulemankohistani786@gmail.com
[2] PhD Scholar,Ibadat International University, Islamabad, wasiurrahmannadvi@gmail.com

تعارف

انسانی معاشرے میں عدل کے قیام، حقوق کے تحفظ اور تنازعات کے منصفانہ حل کے لیے نظام اثبات بنیادی اہمیت رکھتا ہے۔ کسی شخص کا حق، کسی معاملے کی حقیقت یا کسی جرم کا وقوع محض دعویٰ کی بنیاد پر تسلیم نہیں کیا جا سکتا، بلکہ عدالت کو ایسے معتبر ذرائع درکار ہوتے ہیں جن کے ذریعے متنازعہ حقیقت تک رسائی حاصل کی جا سکے۔ اسلامی شریعت نے انسانی حقوق کے تحفظ اور عدل کے قیام کے لیے نظام اثبات کے متعدد اصول بیان کیے ہیں اور شہادت، اقرار، کتابت اور قرائن سمیت مختلف ذرائع کو ان کے متعلقہ شرائط کے ساتھ زیرِ بحث لایا ہے۔ اللہ تعالیٰ کا ارشاد ہے:

يَا أَيُّهَا الَّذِينَ آمَنُوا كُونُوا قَوَّامِينَ بِالْقِسْطِ شُهَدَاءَ لِلَّهِ[3]

اے ایمان والو! انصاف پر مضبوطی سے قائم رہنے والے اور اللہ کے لیے گواہی دینے والے بنو۔

اسی طرح قرآن مجید نے گواہی کو چھپانے سے منع کرتے ہوئے فرمایا:

وَلَا تَكْتُمُوا الشَّهَادَةَ. اور گواہی کو نہ چھپاؤ۔[4]

مالی معاملات میں تحریر، گواہی اور دستاویز بندی کے اہتمام کی ہدایت بھی قرآن مجید میں تفصیل سے موجود ہے:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا تَدَايَنْتُمْ بِدَيْنٍ إِلَىٰ أَجَلٍ مُسَمًّى فَاكْتُبُوهُ... اے ایمان والو! جب تم کسی مقررہ مدت تک آپس میں قرض کا معاملہ کرو تو اسے لکھ لیا کرو۔

ان نصوص سے واضح ہوتا ہے کہ اسلامی نظام قضاء میں حقائق کے درست تعین، حقوق کی حفاظت اور نزاعات کے منصفانہ حل کے لیے معتبر ذرائع اثبات کو بنیادی اہمیت حاصل ہے۔

موجودہ دور میں انفارمیشن ٹیکنالوجی نے انسانی سرگرمیوں کے ریکارڈ کی نوعیت تبدیل کر دی ہے۔ آج کسی شخص کی گفتگو، مالی لین دین، مقام، شناخت، کاروباری سرگرمی، معاہدہ یا کسی واقعے سے متعلق معلومات صرف کاغذی دستاویز یا عینی گواہ کے ذریعے ہی محفوظ نہیں ہوتیں، بلکہ ان کا بڑا حصہ موبائل فون، کمپیوٹر، سرور، کلاؤڈ اسٹوریج، سوشل میڈیا پلیٹ فارم اور دیگر ڈیجیٹل نظاموں میں محفوظ ہوتا ہے۔ چنانچہ عدالتی کارروائی میں روایتی شواہد کے ساتھ ڈیجیٹل مواد کی اہمیت مسلسل بڑھ رہی ہے۔[5]

اس تبدیلی نے قانون اثبات کے سامنے نئے سوالات پیدا کیے ہیں۔ مثال کے طور پر اگر کسی مقدمے میں واٹس ایپ پیغام پیش کیا جائے تو یہ کیسے ثابت ہو گا کہ پیغام واقعی اسی شخص نے بھیجا تھا؟ اگر کوئی آڈیو یا ویڈیو ریکارڈنگ پیش کی جائے تو اس کی اصلیت کیسے ثابت ہو گی؟ اگر کسی موبائل فون سے حاصل شدہ لوکیشن ڈیٹا کسی شخص کے ایک خاص مقام پر موجود ہونے کی نشاندہی کرتا ہو تو اس کی فنی صحت اور نسبت کس طرح متعین ہو گی؟ اسی طرح اسکرین شاٹ، ای میل، CCTV فوٹیج یا سرور لاگ کی اثباتی قوت کیا ہو گی؟

---

[3] القرآن الکریم، النساء 4:135۔

[4] القرآن الکریم، البقرۃ 2:283۔

[5] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Amsterdam: Academic Press, 2011), 7–9.

یہ سوال صرف قانونی نوعیت کے نہیں بلکہ شرعی اعتبار سے بھی اہم ہیں۔ اسلامی نظامِ اثبات میں خبر، شہادت اور قرینے کی قبولیت محض ان کے وجود پر موقوف نہیں بلکہ صدق، علم، عدالت، دلالت، نسبت اور دیگر شرائط سے متعلق ہے۔ رسول اللہ ﷺ نے جھوٹی گواہی کو کبیرہ گناہوں میں شمار فرمایا۔

عَنْ أَبِي بَكْرَةَ رَضِيَ اللَّهُ عَنْهُ قَالَ: قَالَ النَّبِيُّ ﷺ: أَلَا أُنَبِّئُكُمْ بِأَكْبَرِ الْكَبَائِرِ؟» ثَلَاثًا، قَالُوا: بَلَى يَا رَسُولَ اللَّهِ، قَالَ: الْإِشْرَاكُ بِاللَّهِ، وَعُقُوقُ الْوَالِدَيْنِ وَجَلَسَ وَكَانَ مُتَّكِئًا فَقَالَ: أَلَا وَقَوْلُ الزُّورِ قَالَ: فَمَا زَالَ يُكَرِّرُهَا حَتَّى قُلْنَا: لَيْتَهُ سَكَتَ.[6] حضرت ابو بکرہ رضی اللہ عنہ بیان کرتے ہیں کہ نبی کریم ﷺ نے فرمایا'' : کیا میں تمہیں سب سے بڑے کبیرہ گناہوں کے بارے میں نہ بتاؤں؟ ''آپ ﷺ نے یہ بات تین مرتبہ فرمائی۔ صحابہؓ نے عرض کیا: کیوں نہیں، یارسول اللہ! آپ ﷺ نے فرمایا'' :اللہ کے ساتھ شرک کرنا اور والدین کی نافرمانی کرنا۔ ''پھر آپ ﷺ ٹیک لگا کر بیٹھے ہوئے تھے، سیدھے ہو کر بیٹھ گئے اور فرمایا'' :خبردار! جھوٹی بات کہنا (قولِ زور) بھی ''! راوی کہتے ہیں کہ آپ ﷺ اسے بار بار دہراتے رہے، یہاں تک کہ ہم نے دل میں کہا: کاش! آپ ﷺ خاموش ہو جائیں۔

اس سے معلوم ہوتا ہے کہ اسلامی نظامِ اثبات میں کسی بھی معلومات کی ظاہری موجودگی سے زیادہ اس کی صداقت اور حق سے مطابقت اہم ہے۔ اسی تناظر میں ڈیجیٹل شواہد کا مسئلہ سامنے آتا ہے۔ ڈیجیٹل مواد ایک طرف حقائق کے تعین میں انتہائی مفید ثابت ہو سکتا ہے، لیکن دوسری طرف اس میں جعل سازی، ترمیم، غلط نسبت، مصنوعی تخلیق اور غیر مجاز حصول کے امکانات بھی موجود ہیں۔ جدید مصنوعی ذہانت نے اس مسئلے کو مزید پیچیدہ کر دیا ہے، کیونکہ اب ایسی تصاویر، آوازیں اور ویڈیوز تیار کرنا ممکن ہے جو ظاہری طور پر حقیقی معلوم ہوتی ہیں لیکن حقیقت میں مصنوعی یا تبدیل شدہ ہوتی ہیں۔

پاکستانی قانون نے بھی اس تکنیکی تبدیلی کو ملحوظ رکھتے ہوئے برقی شواہد کے لیے قانونی گنجائش پیدا کی ہے۔ قانونِ شہادت آرڈر 1984ء میں بنیادی شہادت کے عمومی اصولوں کے ساتھ جدید معلوماتی نظام سے حاصل شدہ برقی نتائج کے حوالے سے احکام موجود ہیں، جبکہ آرٹیکل 164 عدالت کو جدید آلات اور تکنیک کے ذریعے دستیاب ہونے والی شہادت سے استفادہ کرنے کا اختیار فراہم کرتا ہے۔[7]

اس تحقیق کا بنیادی مقصد یہ ہے کہ ڈیجیٹل شواہد کی شرعی تکییف، حجیت اور اثباتی قوت کو اسلامی اصولِ اثبات کی روشنی میں واضح کیا جائے اور پاکستانی قانونی نظام، بالخصوص قانونِ شہادت آرڈر 1984ء کے آرٹیکلز 73 اور 164 کے ساتھ اس کا تقابلی جائزہ لیا جائے۔ اس کے ساتھ یہ بھی واضح کیا جائے گا کہ ڈیجیٹل شواہد کی قبولیت کے لیے اصلیت، نسبت، سالمیت، تحویل کا تسلسل اور فنی تصدیق کس قدر اہم ہیں۔ تحقیق کا بنیادی سوال یہ نہیں کہ ہر ڈیجیٹل مواد کو ''شہادت'' کہا جا سکتا ہے یا نہیں، بلکہ یہ ہے کہ ڈیجیٹل مواد کی حقیقی فقہی و قانونی حیثیت کیا ہے اور اس کی اثباتی قوت کس بنیاد پر متعین کی جائے گی؟ یہی سوال اس تحقیق کے تمام مباحث کو باہم مربوط کرتا ہے۔

---

[6] محمد بن إسماعيل البخاري، صحيح البخاري، كتاب الشهادات، باب ماقيل في شهادة الزور، حدیث رقم 2654۔

[7] Qanun-e-Shahadat Order, 1984, arts. 73, 164-

ڈیجیٹل شواہد کا لغوی واصطلاحی مفہوم

ڈیجیٹل شواہد کی اصطلاح دو بنیادی اجزا ''ڈیجیٹل'' اور ''شواہد'' سے مرکب ہے۔ ان دونوں کے لغوی واصطلاحی مفاہیم کو الگ الگ واضح کرنا اس اصطلاح کی جامع فقہی و قانونی تفہیم کے لیے ضروری ہے۔

1۔ ڈیجیٹل کا مفہوم:

ڈیجیٹل (Digital) بنیادی طور پر جدید فنی و معلوماتی اصطلاح ہے، جس کا تعلق ایسی معلومات سے ہے جو عددی صورت میں، بالخصوص ثنائی نظام (Binary System) کے ذریعے تخلیق، محفوظ، منتقل، مرتب یا پراسیس کی جاتی ہیں۔ جدید معلوماتی ٹیکنالوجی میں متن، تصویر، آواز، ویڈیو، برقی دستاویزات، ای میل، پیغامات، ویب مواد، موبائل فون کا ڈیٹا، سرور ریکارڈ، جی پی ایس معلومات اور دیگر الیکٹرانک معلومات اسی ڈیجیٹل نظام کی مختلف صورتیں ہیں۔ چنانچہ ''ڈیجیٹل'' سے مراد محض کمپیوٹر یا موبائل سے متعلق کوئی چیز نہیں، بلکہ معلومات کے اس مخصوص برقی وعددی قالب سے ہے جس میں اسے کسی ڈیجیٹل نظام کے ذریعے تخلیق، محفوظ یا منتقل کیا جاتا ہے۔

2۔ شواہد کا لغوی مفہوم:

''شواہد''، ''شاہد'' اور ''شہادت'' عربی مادہ (ش-ہ-د) سے مشتق ہیں۔ عربی لغت میں اس مادے کے بنیادی مفاہیم میں کسی امر کے موقع پر حاضر ہونا، اسے دیکھنا، اس کا مشاہدہ کرنا، اس سے واقف ہونا اور کسی واقعے کے متعلق خبر دینا شامل ہیں۔ ابن منظور لکھتے ہیں کہ ''شہادت'' کے مفہوم میں حضور اور مشاہدہ کے ساتھ کسی امر کے بارے میں علم و خبر دینا بھی شامل ہے۔[8] اس سے واضح ہوتا ہے کہ لغوی اعتبار سے شہادت کا بنیادی تعلق کسی واقعے یا حقیقت کے ادراک اور پھر اس کے بارے میں خبر دینے سے ہے۔

3۔ فقہی اصطلاح میں شہادت:

فقہی اصطلاح میں شہادت محض کسی واقعے کی اطلاع دینے کے مترادف نہیں، بلکہ اس کے لیے مخصوص شرائط اور ایک خاص اثباتی حیثیت پائی جاتی ہے۔ حنفی فقہاء نے شہادت کو حقوق کے اثبات کے لیے عدالت کے سامنے مخصوص طریقے سے سچی خبر دینے سے تعبیر کیا ہے۔ علامہ زیلعی لکھتے ہیں: إخبارُ صِدقٍ لإثباتِ حقٍّ بلفظِ الشهادةِ في مجلسِ القضاءِ[9] مجلسِ قضاء میں لفظِ شہادت کے ذریعے کسی حق کے اثبات کے لیے سچی خبر دینا شہادت ہے۔

اس تعریف سے معلوم ہوتا ہے کہ فقہی مفہوم میں شہادت کے لیے محض معلومات کا وجود کافی نہیں، بلکہ اس میں خبر دینے والا شخص، اس کا متعلقہ واقعے سے علم، سچی خبر، حق کا اثبات اور مجلسِ قضاء میں ادائیگی جیسے عناصر بنیادی حیثیت رکھتے ہیں۔ یہی وجہ ہے کہ ہر قسم کے ڈیجیٹل مواد کو فقہی اصطلاح میں ''شہادت'' قرار دینا درست نہیں ہوگا۔

---

[8] محمد بن مکرم ابن منظور، لسان العرب، مادہ ''شھد''، (بیروت: دار صادر، 1414ھ)، 3:239۔

[9] عثمان بن علي الزيلعي، تبيين الحقائق شرح كنز الدقائق، (القاهرة: المطبعة الكبرى الأميرية، 1313ھ)، 4:206۔

4۔ڈیجیٹل شواہد اور فقہی اصطلاحات کا باہمی تعلق:

ڈیجیٹل مواد کی فقہی تکییف کرتے وقت اس کے ''ڈیجیٹل'' ہونے کو فیصلہ کن حیثیت حاصل نہیں، بلکہ یہ دیکھا جائے گا کہ وہ اثباتِ حق میں کس نوعیت کا کردار ادا کر رہا ہے۔ چنانچہ عدالت میں ویڈیو لنک کے ذریعے کسی شخص کا براہِ راست بیان ہو تو اس کا تعلق انسانی شہادت کے باب سے ہو سکتا ہے، کیونکہ یہاں ایک شخص اپنے علم و مشاہدے کی بنیاد پر خبر دے رہا ہے۔ اس کے برعکس کسی سرور کا خود کار لاگ انسانی شہادت نہیں، بلکہ ایک برقی و فنی ریکارڈ ہے۔ اسی طرح کسی شخص کی جانب سے بھیجا گیا ایسا پیغام جس میں وہ اپنے ذمہ کسی حق یا واقعے کا اعتراف کرتا ہو، اس کی نسبت ثابت ہونے کی صورت میں ''اقرار'' کے مفہوم سے قریب ہو سکتا ہے۔ جبکہ CCTV فوٹیج، GPS لوکیشن، کال ڈیٹیل ریکارڈ، سرور لاگز اور میٹا ڈیٹا وغیرہ عموماً ایسے خارجی آثار اور معلومات ہیں جو کسی واقعے کے وقوع یا عدمِ وقوع پر دلالت کرتے ہیں، اس لیے ان کی فقہی تکییف زیادہ مناسب طور پر **قرائن** کے ضمن میں کی جا سکتی ہے۔

اس تناظر میں یہ اصول قابلِ توجہ ہے کہ ڈیجیٹل شواہد ایک مستقل فقہی قسمِ اثبات کا نام نہیں، بلکہ مختلف نوعیت کے اثباتی مواد کے لیے ایک جامع جدید اصطلاح ہے۔ اس کے تحت آنے والی ہر چیز کی فقہی حیثیت اس کی نوعیت، ماخذ، نسبت، دلالت اور استعمال کے طریقے کے اعتبار سے متعین ہو گی۔ لہٰذا ایک ہی ڈیجیٹل وسیلے میں موجود مختلف مواد کی فقہی تکییف بھی مختلف ہو سکتی ہے؛ مثلاً موبائل فون میں محفوظ تحریر کتابت یا اقرار کے حکم سے متعلق ہو سکتی ہے، جبکہ اسی فون سے حاصل شدہ لوکیشن ڈیٹا قرینہ اور کسی شخص کی براہِ راست ویڈیو گواہی شہادت کے باب سے متعلق ہو سکتی ہے۔

5۔ڈیجیٹل شواہد کی اصطلاحی تعریف:

مذکورہ لغوی، فقہی اور فنی مباحث کی روشنی میں ڈیجیٹل شواہد کی ایک جامع اصطلاحی تعریف اس طرح کی جا سکتی ہے:

''ڈیجیٹل شواہد سے مراد ایسی برقی یا عددی معلومات، تحریر، ریکارڈ، فائل، آڈیو، ویڈیو، تصویری مواد، میٹا ڈیٹا یا کسی ڈیجیٹل نظام سے حاصل ہونے والا ایسا قابلِ فہم مواد ہے جو کسی ڈیجیٹل آلہ، معلوماتی نظام یا برقی ذریعے کے توسط سے تخلیق، محفوظ، منتقل، وصول یا بازیافت ہوا ہو اور کسی قانونی طور پر متعلقہ حق، دعوے، واقعے، جرم یا ذمہ داری کے اثبات یا تردید کے لیے پیش کیا جا سکے، بشرطیکہ اس کی متعلقیت، ماخذ، نسبت، اصلیت، سالمیت اور قابلِ اعتمادیت مناسب ذرائع سے ثابت ہو۔''

اس تعریف کی خصوصیت یہ ہے کہ اس میں ڈیجیٹل شواہد کے فنی وجود اور اثباتی کردار دونوں کو شامل کیا گیا ہے۔ محض یہ امر کہ کوئی معلومات موبائل، کمپیوٹر یا کسی دوسرے ڈیجیٹل آلے میں موجود ہے، اسے خود بخود معتبر شرعی یا قانونی ثبوت نہیں بنا دیتا؛ بلکہ اس کی حجیت اور اثباتی قوت کا تعین اس بات سے ہو گا کہ وہ کس ماخذ سے حاصل ہوئی، کس شخص یا نظام کی طرف منسوب ہے، اس میں کوئی تبدیلی یا تحریف تو نہیں ہوئی، متعلقہ واقعے سے اس کا کیا تعلق ہے اور اسے قابلِ اعتماد فنی و قانونی طریقے سے عدالت یا متعلقہ فورم کے سامنے کس طرح پیش کیا گیا ہے۔

چنانچہ ڈیجیٹل شواہد کے مفہوم میں بالخصوص ماخذ، متعلقیت، نسبت، اصلیت، سالمیت اور قابلِ اعتمادیت بنیادی عناصر کی حیثیت رکھتے ہیں۔ ماخذ سے مراد یہ ہے کہ معلومات کس آلے یا نظام سے حاصل ہوئی؛ متعلقیت سے مراد یہ ہے کہ اس کا زیرِ بحث دعوے یا واقعے سے حقیقی تعلق موجود ہو؛ نسبت سے مراد یہ ہے کہ اسے متعلقہ شخص، آلہ یا نظام کی طرف درست طور پر منسوب کیا جا سکے؛ اصلیت سے مراد یہ ہے کہ پیش

کردہ مواد اپنے اصل ماخذ سے متعلق ہو؛ سالمیت سے مراد یہ ہے کہ اس کے حصول، منتقلی اور پیشی کے دوران اس میں غیر مجاز تبدیلی نہ ہوئی ہو؛ جبکہ قابل اعتمادیت سے مراد اس کی تخلیق، محفوظ رکھنے اور بازیافت کے طریقۂ کار کی فنی و قانونی اعتبار سے اطمینان بخش صحت ہے۔

اس طرح ''ڈیجیٹل شواہد'' کی اصطلاح کو محض جدید ٹیکنالوجی سے پیدا ہونے والے مواد تک محدود کرنا درست نہیں، بلکہ اسے اثباتِ حق کے لیے استعمال ہونے والے ایسے ڈیجیٹل مواد کے مجموعے کے طور پر سمجھنا زیادہ مناسب ہے جس کی شرعی و قانونی حیثیت اس کے فنی وسیلے کے بجائے اس کے حقیقی اثباتی کردار، نسبت، صداقت، سالمیت اور دلالت کی بنیاد پر متعین ہوتی ہے۔ یہی اصول اسلامی قانونِ اثبات اور پاکستانی قانونِ شہادت کے مابین ڈیجیٹل شواہد کے تقابلی مطالعے کے لیے بنیادی نظریاتی نقطۂ آغاز فراہم کرتا ہے۔

ڈیجیٹل شواہد اور روایتی شواہد میں امتیاز

ڈیجیٹل شواہد اور روایتی شواہد کے درمیان بنیادی امتیاز ان کی وجودی ساخت، تخلیق و حفاظت کے طریقۂ کار، ظاہری صورت، نسبت کے تعین اور صداقت و سالمیت کی جانچ سے متعلق ہے۔ روایتی مادی شواہد عموماً ایسی محسوس اور قابلِ مشاہدہ اشیاء پر مشتمل ہوتے ہیں جنہیں براہِ راست دیکھا، چھوا یا محفوظ کیا جا سکتا ہے؛ مثلاً کاغذی دستاویز، دستخط شدہ معاہدہ، کسی جرم میں استعمال ہونے والی مادی چیز، تحریری ریکارڈ یا دیگر مادی آثار۔ اس کے برعکس ڈیجیٹل شواہد اپنی اصل میں برقی و عددی معلومات پر مشتمل ہوتے ہیں، جو عموماً کمپیوٹر، موبائل فون، سرور، کیمرہ، میموری کارڈ یا کسی دوسرے ڈیجیٹل نظام میں مخصوص فنی قالب کے تحت محفوظ رہتی ہیں۔ صارف یا عدالت کے سامنے جو متن، تصویر، آواز یا ویڈیو ظاہر ہوتی ہے، وہ دراصل اس بنیادی ڈیجیٹل ڈیٹا کا قابلِ فہم اظہار ہوتی ہے؛ اس لیے اس کا ظاہری مشاہدہ اور اس کے اصل ڈیجیٹل ماخذ کا ثبوت دو الگ امور ہیں۔[10]

روایتی دستاویز میں اس کی مادی صورت بسا اوقات ثبوت کی شناخت اور حفاظت میں معاون ہوتی ہے، جبکہ ڈیجیٹل دستاویز میں اصل اور اس کی نقل کے درمیان ظاہری فرق ہمیشہ نمایاں نہیں ہوتا۔ مثلاً کسی کاغذی معاہدے کے اصل نسخے پر موجود کاغذ، سیاہی، دستخط اور دیگر مادی خصوصیات اس کی شناخت اور جانچ میں معاون ہو سکتی ہیں، لیکن کسی موبائل فون پر دکھائی دینے والا واٹس ایپ پیغام یا کمپیوٹر اسکرین پر ظاہر ہونے والی کوئی برقی دستاویز محض اس ظاہری شکل کی بنیاد پر اپنے اصل ماخذ، تخلیق کنندہ، تاریخ و وقت یا عدمِ تحریف کو قطعی طور پر ثابت نہیں کرتی۔ اسی طرح کسی تصویر، آڈیو یا ویڈیو فائل کا چل جانا یا قابلِ مشاہدہ ہونا اس امر کا لازمی ثبوت نہیں کہ وہ اصل فائل ہے، مکمل طور پر غیر متبدل ہے یا اس کی نسبت جس شخص یا واقعے کی طرف کی جا رہی ہے وہ درست ہے۔[11]

ڈیجیٹل شواہد کی اس خصوصیت کے باعث ان کی اصلیت (Authentication) اور سالمیت (Integrity) کی جانچ بنیادی اہمیت اختیار کر جاتی ہے۔ اصالت سے مراد یہ تعین کرنا ہے کہ پیش کردہ ڈیجیٹل مواد واقعی اسی شخص، آلے، نظام یا ماخذ سے متعلق ہے جس کی طرف اسے منسوب کیا جا رہا ہے، جبکہ سالمیت سے مراد یہ ہے کہ ثبوت کے حصول، منتقلی، ذخیرے اور پیشی کے دوران اس میں غیر مجاز تبدیلی، حذف یا اضافہ نہیں ہوا۔ اسی طرح تحویل کا تسلسل (Chain of Custody) اس امر کی دستاویزی نگرانی کا نام ہے کہ ڈیجیٹل ثبوت کس

[10] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Waltham, MA: Academic Press, 2011), 7–10-

[11] Simson Garfinkel, "Digital Forensics Research: The Next 10 Years," Digital Investigation 7 (2010): S64–S73-

مقام اور کس ذریعے سے حاصل ہوا، کس شخص یاادارے نے اسے تحویل میں لیا، کس طریقے سے محفوظ کیا گیا، کن مراحل سے گزرااور آخر کار عدالت یامتعلقہ فورم کے سامنے کس حالت میں پیش کیا گیا۔ان مراحل میں کسی غیر واضح یا غیر مستند تبدیلی سے ثبوت کی قابل اعتمادیت متاثر ہو سکتی ہے۔[12]

اس فرق کا ایک اہم پہلو نقل پذیری (Reproducibility) ہے۔روایتی مادی شواہد کی نقل اور اصل کے درمیان عموماً مادی فرق موجود رہتا ہے، جبکہ ڈیجیٹل فائل کی ایک درست نقل بسااوقات ظاہری طور پر اصل فائل سے بالکل مشابہ ہوتی ہے۔یہی خصوصیت ڈیجیٹل شواہد کو ایک طرف محفوظ اور باآسانی منتقل کیے جانے کے قابل بناتی ہے، لیکن دوسری طرف یہ سوال بھی پیدا کرتی ہے کہ عدالت کے سامنے پیش کیا جانے والا مواد اصل ماخذ سے کس درجے میں منسلک ہے۔چنانچہ ڈیجیٹل شواہد میں صرف ''مواد کیا ہے؟'' کا سوال کافی نہیں، بلکہ یہ بھی دیکھا جاتا ہے کہ **یہ مواد کہاں سے آیا، کس نے تخلیق کیا، کس آلے یا نظام میں محفوظ رہا، اس کی نسبت کس شخص سے ہے، اس میں کوئی تبدیلی ہوئی یا نہیں، اور اس کی موجودہ شکل اصل ڈیٹا سے کس حد تک مطابقت رکھتی ہے۔[13]

مزید برآں، روایتی اور ڈیجیٹل شواہد کے درمیان ایک نمایاں فرق میٹاڈیٹا (Metadata) اور پوشیدہ فنی معلومات کا ہے۔بعض ڈیجیٹل فائلوں کے ساتھ ایسی معلومات بھی محفوظ ہوتی ہیں جو عام صارف کو براہِ راست نظر نہیں آتیں، مثلاً فائل کی تخلیق یا ترمیم کا وقت، فائل کا حجم، مقام سے متعلق معلومات، ڈیوائس کی تفصیلات یا دیگر تکنیکی خصوصیات۔یہ معلومات کسی ڈیجیٹل ثبوت کی نسبت، زمانی ترتیب اور سالمیت کی جانچ میں معاون ہو سکتی ہیں، تاہم محض میٹاڈیٹا کی موجودگی کسی واقعے کے بارے میں قطعی نتیجہ اخذ کرنے کے لیے ہر صورت میں کافی نہیں ہوتی؛ اس کی دلالت کو دیگر شواہد اور فنی جانچ کے ساتھ پرکھنا ضروری ہے۔[14]

اسی طرح ڈیجیٹل شواہد میں تغیر پذیری (Volatility) کا عنصر بھی اہم ہے۔بعض ڈیجیٹل معلومات، خصوصاً عارضی یا متحرک ڈیٹا، محدود مدت تک دستیاب رہتی ہیں یا کسی نظام کے استعمال، بند ہونے، دوبارہ شروع ہونے یا دیگر فنی عوامل کے نتیجے میں تبدیل یا ضائع ہو سکتی ہیں۔اس لیے ڈیجیٹل ثبوت کے حصول میں تاخیر یا غیر محتاط طریقۂ کار اس کی اصل حالت کو متاثر کر سکتا ہے۔یہی وجہ ہے کہ ڈیجیٹل فارنزک میں اصل ڈیٹا کو محفوظ رکھنے، اس کی قابل اعتماد نقل تیار کرنے اور تجزیے کے عمل کو اس طرح انجام دینے پر زور دیا جاتا ہے کہ اصل شواہد میں غیر ضروری تبدیلی نہ آئے۔[15]

فقہی اعتبار سے بھی یہ امتیاز نہایت اہم ہے۔روایتی یا ڈیجیٹل ہونا بذاتِ خود کسی ثبوت کی شرعی حجیت کا فیصلہ نہیں کرتا، بلکہ اصل سوال یہ ہے کہ وہ مواد شہادت، اقرار، کتابت، قرینہ یا کسی دوسرے معتبر طریقۂ اثبات میں سے کس نوعیت کا ہے اور اس کی نسبت و صداقت کس درجے

---

[12] Karen Kent et al., Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86 (Gaithersburg, MD: National Institute of Standards and Technology, 2006), 33–38-

[13] ISO/IEC 27037:2012, Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (Geneva: International Organization for Standardization, 2012), 1–4-

[14] Eoghan Casey, Digital Evidence and Computer Crime, 3rd ed., 95–101-

[15] National Institute of Standards and Technology, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1 (Gaithersburg, MD: NIST, 2014), 1–6-

میں ثابت ہے۔ مثلاً کاغذ پر لکھی ہوئی تحریر اور ڈیجیٹل صورت میں محفوظ تحریر دونوں کتابت کے مفہوم سے متعلق ہو سکتی ہیں، لیکن ان کی نسبت اور اصالت ثابت کرنے کے ذرائع مختلف ہو سکتے ہیں۔ اسی طرح CCTV فوٹیج، GPS ریکارڈ یا سرور لاگ اپنی فنی ساخت کے اعتبار سے روایتی انسانی شہادت کے مانند نہیں، بلکہ عموماً قرائن یا فنی ریکارڈ کے طور پر زیرِ بحث آئیں گے۔ اسلامی قانونِ اثبات میں بھی قرائن کو ان کی دلالت اور قوت کے اعتبار سے جانچا جاتا ہے، اس لیے کسی جدید فنی وسیلے کی شرعی حیثیت متعین کرتے وقت اس کے حقیقی اثباتی کردار کو سامنے رکھنا ضروری ہے۔[16]

اس بنا پر ڈیجیٹل شواہد اور روایتی شواہد کے درمیان فرق کو محض ''مادی'' اور ''غیر مادی'' کی تقسیم تک محدود کرنا درست نہیں ہوگا۔ اصل امتیاز یہ ہے کہ ڈیجیٹل ثبوت کی تخلیق، ذخیرہ، نقل، بازیافت، نسبت، تصدیق اور سالمیت زیادہ تر فنی نظام اور مخصوص تکنیکی طریقۂ کار سے وابستہ ہوتی ہے۔ چنانچہ عدالت یا شرعی فورم کے سامنے اس کی قدر و قیمت متعین کرتے وقت مواد کے ظاہری وجود کے ساتھ اس کے اصل ماخذ، نسبت، فنی سالمیت، تحویل کے تسلسل، فارنزک جانچ، متعلقہ واقعے سے تعلق اور دیگر مؤید شواہد کو بھی ملحوظ رکھنا ضروری ہے۔ یوں ڈیجیٹل شواہد جدید ٹیکنالوجی کے نتیجے میں پیدا ہونے والی ایک نئی اثباتی صورت ضرور ہیں، لیکن ان کی شرعی و قانونی تکییف بنیادی طور پر انہی اصولوں کے تحت کی جائے گی جن میں ثبوت کی نسبت، صداقت، دلالت اور اعتمادیت بنیادی اہمیت رکھتے ہیں۔

ڈیجیٹل شواہد کی اہم اقسام

ڈیجیٹل شواہد مختلف ذرائع اور فنی صورتوں میں پائے جاتے ہیں اور ان کی اثباتی قدر و حجیت کا تعین ان کی نوعیت، ماخذ، نسبت، سالمیت اور متعلقہ واقعے سے تعلق کی بنیاد پر کیا جاتا ہے۔ ان میں سب سے اہم برقی مراسلات اور پیغامات ہیں، جن میں ای میل، ایس ایم ایس، واٹس ایپ، ٹیلی گرام اور دیگر مواصلاتی ذرائع شامل ہیں۔ یہ کسی معاہدے، اقرار، مالی معاملے، دھمکی یا باہمی رابطے کے اثبات میں معاون ہو سکتے ہیں، تاہم ان کی نسبت، تخلیق یا ارسال کا وقت، اصل ماخذ اور عدمِ تحریف کی تصدیق ضروری ہے۔ اسی طرح برقی دستاویزات میں الیکٹرانک معاہدات، رسیدیں، انوائسز، بینکاری ریکارڈ، اکاؤنٹنگ فائلیں، سرکاری برقی ریکارڈ اور برقی دستخط شامل ہیں، جو جدید تجارتی، مالی اور انتظامی معاملات میں اہم اثباتی مواد فراہم کرتے ہیں۔ آڈیو اور ویڈیو ریکارڈنگ، مثلاً CCTV فوٹیج، موبائل ویڈیوز اور صوتی ریکارڈنگ، کسی شخص کی موجودگی، کسی واقعے کے وقوع یا کسی گفتگو کے بارے میں معلومات فراہم کر سکتی ہیں، لیکن ان کی اصلیت، مکمل ہونے اور عدمِ تحریف کی فنی جانچ ضروری ہے۔ موبائل فون اور کمپیوٹر سے حاصل شدہ ڈیٹا میں کال ریکارڈ، تصاویر، ویڈیوز، رابطہ فہرست، براؤزر ہسٹری، ایپلی کیشن ڈیٹا، محفوظ شدہ فائلیں اور بعض صورتوں میں حذف شدہ معلومات شامل ہیں، جو کسی معاملے میں اہم قرائن فراہم کر سکتی ہیں۔ اسی طرح لوکیشن اور نیٹ ورک ریکارڈ، مثلاً GPS معلومات، IP ایڈریس، سیل سائٹ معلومات، سرور لاگز اور ایکسیس لاگز، کسی آلے یا صارف کی سرگرمی، مقام اور زمانی ترتیب کے تعین میں معاون ہو سکتے ہیں۔ مزید برآں میٹاڈیٹا (Metadata) کسی ڈیجیٹل فائل یا ریکارڈ سے متعلق اضافی فنی معلومات پر مشتمل ہوتا ہے، مثلاً تخلیق یا ترمیم کا وقت، فائل کی نوعیت، حجم اور بعض اوقات آلے یا مقام سے متعلق معلومات؛ یہ کسی ڈیجیٹل مواد کے ماخذ، زمانی ترتیب اور سالمیت کی جانچ

---

[16] ابن القیم الجوزیۃ، الطرق الحکمیۃ فی السیاسۃ الشرعیۃ (بیروت: دار الکتب العلمیۃ، 1415ھ)، 9–15

میں معاون ہو سکتا ہے، تاہم اس کی اثباتی قدر کا تعین دیگر شواہد اور فنی جانچ کے ساتھ کیا جائے گا۔[17] یوں ڈیجیٹل شواہد کی یہ تمام اقسام اپنی فنی ساخت میں مختلف ہونے کے باوجود ایک مشترک خصوصیت رکھتی ہیں کہ ان کی شرعی و قانونی حیثیت محض ڈیجیٹل وجود سے نہیں بلکہ ماخذ، نسبت، متعلقیت، اصلیت، سالمیت اور قابلِ اعتمادیت کی تحقیق کے بعد متعین ہوتی ہے۔

ڈیجیٹل شواہد کی بنیادی خصوصیات

ڈیجیٹل شواہد اپنی فنی اور برقی ساخت کے باعث روایتی شواہد سے بعض نمایاں خصوصیات میں مختلف ہوتے ہیں۔ ان کی پہلی اہم خصوصیت آسان نقل پذیری ہے؛ ایک ہی ڈیجیٹل فائل کی متعدد نقول بآسانی تیار کی جاسکتی ہیں اور بظاہر وہ اصل فائل سے یکساں دکھائی دے سکتی ہیں۔ اس کے برعکس محض نقل کے وجود سے اس کے اصل ماخذ، تخلیق کار اور سالمیت کا قطعی تعین نہیں ہوتا۔ دوسری اہم خصوصیت تبدیلی پذیری ہے، کیونکہ ڈیجیٹل تصویر، آڈیو، ویڈیو، متن اور دیگر فائلوں میں فنی ذرائع سے ترمیم یا تبدیلی ممکن ہوتی ہے، اس لیے ان کی اصالت اور سالمیت کی فنی جانچ ضروری ہوتی ہے۔ تیسری خصوصیت کثرتِ معلومات ہے؛ ایک موبائل فون، کمپیوٹر یا سرور میں بہت بڑی مقدار میں مختلف نوعیت کا ڈیٹا محفوظ ہو سکتا ہے، جس میں متعلقہ واقعے سے براہِ راست اور بالواسطہ دونوں طرح کی معلومات شامل ہو سکتی ہیں۔ چوتھی خصوصیت بازیافت پذیری ہے؛ بعض حالات میں حذف شدہ یا بظاہر ضائع شدہ معلومات بھی مناسب فرانزک طریقوں کے ذریعے بازیافت کی جاسکتی ہیں۔ پانچویں اہم خصوصیت خودکار تخلیق ہے؛ بعض ڈیجیٹل ریکارڈ کسی شخص کے براہِ راست تحریری یا زبانی اقدام کے بغیر خودکار نظام کے ذریعے وجود میں آتے ہیں، مثلاً سرور لاگز، بینکاری لین دین کے ریکارڈ، رسائی کے لاگز اور بعض CCTV ریکارڈز۔ اسی طرح ڈیجیٹل شواہد کی ایک اہم خصوصیت تکنیکی وابستگی بھی ہے، کیونکہ ان کی شناخت، تشریح اور تصدیق کے لیے عموماً متعلقہ آلہ، نظام، سافٹ ویئر، میٹاڈیٹا اور دیگر فنی معلومات کو ملحوظ رکھنا پڑتا ہے۔[18]

ان خصوصیات کی بنا پر ڈیجیٹل شواہد کی قانونی یا شرعی حیثیت متعین کرتے وقت صرف اس بات پر اکتفا نہیں کیا جاسکتا کہ کوئی معلومات کسی اسکرین، موبائل یا کمپیوٹر میں موجود ہے، بلکہ اس کے ماخذ، نسبت، متعلقیت، اصالت، سالمیت، حصول کے طریقۂ کار اور محفوظ رکھنے کے مراحل کی بھی تحقیق ضروری ہے۔ خصوصاً یہ معلوم کرنا اہم ہوتا ہے کہ ثبوت کس ذریعے سے حاصل کیا گیا، کس شخص یا ادارے نے اسے حاصل کیا، اس کی تحویل اور حفاظت کس طریقے سے ہوئی، دورانِ حصول یا منتقلی اس میں کوئی تبدیلی تو نہیں ہوئی، اور کیا اس کی فنی طور پر قابلِ اعتماد تصدیق ممکن ہے۔ ڈیجیٹل فرانزک کے بین الاقوامی معیارات بھی اسی مقصد کے لیے شواہد کی شناخت، حصول، تحویل اور حفاظت کے منظم اصول بیان کرتے ہیں، تاکہ ثبوت کی سالمیت (Integrity) برقرار رہے اور عدالت اس کی اثباتی قدر کا مناسب انداز میں جائزہ لے سکے۔[19]

---

[17] Karen Kent et al., Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86

[18] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Waltham, MA: Academic Press, 2011), 7–10.

[19] International Organization for Standardization, ISO/IEC 27037:2012: Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (Geneva: ISO, 2012), 1–4.

یہ خصوصیات اس امر کی بھی وضاحت کرتی ہیں کہ ڈیجیٹل شواہد کو محض ان کی ڈیجیٹل صورت کی بناپر قطعی اور حتمی ثبوت قرار نہیں دیا جاسکتا؛ بلکہ ان کی حجیت اور اثباتی قدر کا تعین ان کے حقیقی ماخذ، نسبت، فنی تصدیق، سالمیت اور واقعے سے تعلق کی مجموعی تحقیق کے بعد کیا جائے گا۔ یہی اصول شرعی نقطۂ نظر سے بھی اہم ہے، کیونکہ کسی ڈیجیٹل مواد کی شرعی تکییف اس کی ظاہری شکل کے بجائے اس کی حقیقت، ماخذ اور ثبوت کے طور پر اس کے کردار کی بنیاد پر ہوگی۔

اسلامی قانونِ اثبات میں شہادت اور ڈیجیٹل شواہد

اسلامی نظامِ قضاء میں شہادت اثباتِ حقوق کا ایک بنیادی ذریعہ ہے۔ قرآن مجید نے ادائے شہادت کو عدل وانصاف کے ساتھ مربوط کیا اور گواہی کو درست طور پر ادا کرنے کی تاکید فرمائی۔ ارشادِ باری تعالیٰ ہے:

وَأَقِيمُوا الشَّهَادَةَ لِلّٰهِ[20] اللہ کے لیے گواہی کو قائم کرو۔

سی طرح رسول اللہ ﷺ نے جھوٹی گواہی اور قولِ زور کو کبیرہ گناہوں میں شمار فرمایا۔ حضرت ابو بکرہ رضی اللہ عنہ سے روایت ہے کہ نبی کریم ﷺ نے فرمایا:

عَنْ أَبِي بَكْرَةَ رَضِيَ اللَّهُ عَنْهُ قَالَ: قَالَ النَّبِيُّ ﷺ: «أَلَا أُنَبِّئُكُمْ بِأَكْبَرِ الْكَبَائِرِ؟» ثَلَاثًا، قَالُوا: بَلَى يَا رَسُولَ اللَّهِ، قَالَ: الْإِشْرَاكُ بِاللَّهِ، وَعُقُوقُ الْوَالِدَيْنِ وَجَلَسَ وَكَانَ مُتَّكِئًا فَقَالَ: أَلَا وَقَوْلُ الزُّورِ قَالَ: فَمَا زَالَ يُكَرِّرُهَا حَتَّى قُلْنَا: لَيْتَهُ سَكَتَ.[21] حضرت ابو بکرہ رضی اللہ عنہ بیان کرتے ہیں کہ نبی کریم ﷺ نے فرمایا'' : کیا میں تمہیں سب سے بڑے کبیرہ گناہوں کے بارے میں نہ بتاؤں؟ ''آپ ﷺ نے یہ بات تین مرتبہ فرمائی۔ صحابہؓ نے عرض کیا: کیوں نہیں، یارسول اللہ! آپ ﷺ نے فرمایا'' :اللہ کے ساتھ شرک کرنا اور والدین کی نافرمانی کرنا۔ ''پھر آپ ﷺ ٹیک لگا کر بیٹھے ہوئے تھے، سیدھے ہو کر بیٹھ گئے اور فرمایا'' :خبردار! جھوٹی بات کہنا (قولِ زور) بھی ''! راوی کہتے ہیں کہ آپ ﷺ اسے بار بار دہراتے رہے، یہاں تک کہ ہم نے دل میں کہا: کاش! آپ ﷺ خاموش ہو جائیں۔

فقہی تعریفات کے مطالعے سے معلوم ہوتا ہے کہ شہادت میں انسانی علم، ادراک اور خبر کا عنصر بنیادی حیثیت رکھتا ہے۔ حنفی فقہ میں شہادت سے مراد مجلسِ قضاء میں کسی حق کے اثبات کے لیے لفظِ شہادت کے ذریعے سچی خبر دینا ہے۔[3] اس بناپر ہر اس مواد کو جو عدالت میں پیش کیا جائے، محض اس وجہ سے اصطلاحی شہادت قرار نہیں دیا جاسکتا کہ وہ کسی واقعے کے اثبات میں معاون ہے۔ ڈیجیٹل مواد کی شرعی تکییف اس کے حقیقی ماخذ اور اثباتی کردار کی بنیاد پر ہوگی۔

مثلاً اگر کوئی شخص عدالت میں ویڈیو کانفرنس کے ذریعے کسی واقعے کے متعلق اپنا مشاہدہ بیان کرتا ہے تو اصل دلیل اس شخص کی انسانی شہادت ہے، جبکہ ویڈیو کانفرنس اس شہادت کی ادائیگی اور ترسیل کا ذریعہ ہے۔ اس کے برعکس اگر عدالت میں کسی سرور کا خودکار لاگ، کسی نظام کا

---

[20] القرآن الکریم، النساء 4:135۔

[21] محمد بن إسماعيل البخاري، صحيح البخاري، كتاب الشهادات، باب ماقيل في شهادة الزور، حدیث رقم 2654۔

access log یا کسی مشین سے پیدا ہونے والا تکنیکی ریکارڈ پیش کیا جائے تو وہ انسانی شہادت کے مفہوم میں داخل نہیں ہوگا، بلکہ اس کی فقہی تکییف کتابت، دستاویزی ریکارڈ یا قرینہ کے طور پر، اس کی حقیقت اور حالات کے مطابق کی جائے گی۔

اس سے یہ بنیادی اصول سامنے آتا ہے کہ ڈیجیٹل ذریعہ اور شرعی دلیل ایک ہی چیز نہیں ہیں؛ ڈیجیٹل ذریعہ کسی شرعی دلیل کو منتقل، محفوظ یا ظاہر کرنے کا وسیلہ ہو سکتا ہے۔

کتابت اور ڈیجیٹل دستاویز

اسلامی شریعت نے مالی معاملات میں کتابت کو خصوصی اہمیت دی ہے۔ آیتِ دین میں اللہ تعالیٰ نے قرض کے معاملے کو لکھنے کی ہدایت فرمائی:

فَاكْتُبُوهُ[22] اسے لکھ لیا کرو۔

آیتِ دین میں کتابت کا مقصد محض تحریر پیدا کرنا نہیں بلکہ معاملے، ذمہ داری اور حق کو محفوظ طریقے سے ثبت کرنا ہے، تاکہ مستقبل میں نزاع کی صورت میں اس سے رجوع کیا جا سکے۔

اگرچہ عہدِ نزول میں کتابت کے ذرائع کاغذ، صحیفہ، رق اور دیگر مادی وسائل پر مشتمل تھے، لیکن جدید دور میں تحریری معلومات کے اظہار اور محفوظ کرنے کے ذرائع تبدیل ہو چکے ہیں۔ اب الیکٹرانک معاہدات، ای میلز، ڈیجیٹل رسیدیں، بینکاری ریکارڈ، الیکٹرانک دستاویزات اور برقی دستخط اسی نوع کے جدید ذرائع ہیں جن کے ذریعے کسی معاملے کی تحریری صورت محفوظ کی جاتی ہے۔

فقہی تکییف میں اس امر کو بنیادی اہمیت حاصل ہوگی کہ ڈیجیٹل دستاویز میں کسی شخص کی طرف سے کسی حق، ذمہ داری یا معاملے کا تحریری اظہار موجود ہے یا نہیں، وہ تحریر کس شخص کی طرف منسوب ہے، اور اس نسبت و تحریر کی صحت کس حد تک ثابت ہے۔ چنانچہ ڈیجیٹل دستاویز کو کتابت کے جدید وسیلے کے طور پر زیرِ بحث لایا جا سکتا ہے، تاہم اس کی حجیت کا انحصار صرف اس کے ڈیجیٹل وجود پر نہیں بلکہ اس کی نسبت، صحت، سالمیت اور قابلِ اعتمادیت پر ہوگا۔

اقرار اور ڈیجیٹل مواد

اسلامی قانون اثبات میں اقرار کو اثباتِ حق کے اہم ذرائع میں شمار کیا گیا ہے۔ اقرار کی بنیاد یہ ہے کہ کسی شخص کی طرف سے اپنے خلاف کسی حق یا ذمہ داری کا اعتراف ثابت ہو۔ فقہی اصول کے مطابق انسان کا اپنے خلاف حق کا اعتراف دیگر خارجی قرائن کے مقابلے میں خصوصی اثباتی اہمیت رکھتا ہے۔

عصرِ حاضر میں اقرار صرف زبانی گفتگو تک محدود نہیں رہا بلکہ تحریری اور ڈیجیٹل ذرائع سے بھی سامنے آ سکتا ہے۔ مثلاً کسی شخص کی طرف سے ای میل، WhatsApp پیغام، ٹیکسٹ میسج یا کسی دوسرے ڈیجیٹل ذریعے کے توسط سے کسی قرض، مالی ذمہ داری، معاہدے یا کسی واقعے کا واضح اعتراف سامنے آئے تو اصولی طور پر اسے ڈیجیٹل اقرار کے تناظر میں زیرِ بحث لایا جا سکتا ہے۔

تاہم یہاں بنیادی مسئلہ نسبتِ اقرار کا ہے۔ محض کسی شخص کے نام، موبائل نمبر، ای میل ایڈریس یا سوشل میڈیا اکاؤنٹ سے منسوب پیغام کا موجود ہونا لازماً یہ ثابت نہیں کرتا کہ وہ پیغام اسی شخص نے بھیجا تھا۔ اکاؤنٹ کسی دوسرے شخص کے استعمال میں ہو سکتا ہے، شناختی معلومات

[22] القرآن الکریم، البقرۃ 2:282۔

کا غلط استعمال ہو سکتا ہے، یا ڈیجیٹل مواد میں بعد ازاں ترمیم کی جا سکتی ہے۔ اس لیے ڈیجیٹل اقرار کی اثباتی قوت متعین کرنے کے لیے نسبت، اصالت (Authenticity)، سالمیت (Integrity)، حصول کے طریقے اور دیگر متعلقہ حالات کی تحقیق ضروری ہو گی۔

قرائن اور ڈیجیٹل شواہد

ڈیجیٹل شواہد کی فقہی تکییف میں **قرینہ** کو خصوصی اہمیت حاصل ہے۔ قرینہ کسی ایسے ظاہر یا خارجی امر کو کہا جاتا ہے جو اپنے متعلق امر کے ساتھ تعلق کی وجہ سے کسی پوشیدہ حقیقت یا مطلوب معنی کی طرف رہنمائی کرے۔ علامہ جرجانی نے قرینہ کو ایسے امر سے تعبیر کیا ہے جو اپنے متعلق امر کے ساتھ تعلق کی وجہ سے مطلوب معنی کی طرف رہنمائی کرتا ہے۔[23]

قرآن مجید میں حضرت یوسف علیہ السلام کے واقعے میں قمیص کے پھٹنے کی سمت کو حقیقت معلوم کرنے کے لیے استعمال کیا گیا:

إِنْ كَانَ قَمِيصُهُ قُدَّ مِنْ قُبُلٍ فَصَدَقَتْ وَهُوَ مِنَ الْكَاذِبِينَ ۝ وَإِنْ كَانَ قَمِيصُهُ قُدَّ مِنْ دُبُرٍ فَكَذَبَتْ وَهُوَ مِنَ الصَّادِقِينَ[24]

اس آیت سے کم از کم یہ اصول واضح ہوتا ہے کہ کسی خارجی اثر یا علامت کے ذریعے کسی پوشیدہ حقیقت تک استدلالی رسائی ممکن ہے۔

ابن القیم نے بھی قضائی نظام میں قرائن اور حالات کی اہمیت پر تفصیلی بحث کی ہے اور حق تک رسائی کے لیے حالات و قرائن کو نظر انداز کرنے کے خلاف استدلال کیا ہے۔[25]

جدید ڈیجیٹل ماحول میں CCTV footage، GPS data، call records، server logs، access logs اور metadata اسی نوع کے خارجی شواہد کے طور پر بعض مقدمات میں زیرِ غور آ سکتے ہیں۔

البتہ تمام ڈیجیٹل قرائن کی اثباتی قوت یکساں نہیں ہو گی۔ ایک غیر مصدقہ screenshot کے مقابلے میں اصل نظام سے حاصل کیا گیا محفوظ server log زیادہ قابلِ اعتماد ہو سکتا ہے، جبکہ متعدد مستقل ذرائع سے حاصل ہونے والے ایسے ڈیجیٹل ریکارڈ جو ایک دوسرے کی تائید کریں، مجموعی طور پر واقعے کی نسبت اور وقوع پر زیادہ مضبوط دلالت پیدا کر سکتے ہیں۔ اس لیے کسی ڈیجیٹل قرینے کی قوت کا فیصلہ اس کے ماخذ، نسبت، طریقۂ حصول، سالمیت، دلالت اور دیگر شواہد سے مطابقت کی بنیاد پر کیا جائے گا۔

چنانچہ اصولی طور پر کہا جا سکتا ہے کہ ڈیجیٹل شواہد کی شرعی حجیت ان کی محض تکنیکی صورت سے نہیں بلکہ ان کی دلالت، نسبت، صداقت، سالمیت اور مؤید قرائن سے متعین ہو گی۔

اسلامی نظامِ اثبات میں تحقیق و تثبت

اسلامی شریعت نے کسی خبر یا دعوے کو قبول کرنے سے قبل تحقیق، تثبت اور تبین کو بنیادی اصول قرار دیا ہے۔ اللہ تعالیٰ کا ارشاد ہے:

يَا أَيُّهَا الَّذِينَ آمَنُوا إِنْ جَاءَكُمْ فَاسِقٌ بِنَبَإٍ فَتَبَيَّنُوا[26] اے ایمان والو! اگر کوئی فاسق تمہارے پاس کوئی خبر لائے تو تحقیق کر لیا کرو۔

---

[23] علي بن محمد الجرجاني، التعريفات (بيروت: دار الكتب العلمية، 1983)، 174۔

[24] القرآن الکریم، یوسف 12:26–27۔

[25] محمد بن أبي بكر ابن قيم الجوزية، الطرق الحكمية في السياسة الشرعية (القاهرة: مكتبة السنة المحمدية، 1961)، 3–6۔

[26] القرآن الکریم، الحجرات 49:6۔

یہ قرآنی اصول ڈیجیٹل شواہد کے باب میں خصوصی اہمیت رکھتا ہے، کیونکہ جدید ٹیکنالوجی نے معلومات کی تخلیق، ترمیم اور ترسیل کو انتہائی آسان بنادیا ہے۔ چنانچہ کسی تصویر، ویڈیو، آڈیو، اسکرین شاٹ، ای میل یا پیغام کو محض اس بنیاد پر معتبر نہیں سمجھا جاسکتا کہ وہ کسی ڈیجیٹل وسیلے میں موجود ہے۔ اس کے ماخذ اور نسبت کی تحقیق ضروری ہے۔

ڈیجیٹل مواد کی تحقیق میں کم از کم درج ذیل امور کو ملحوظ رکھنا ضروری ہوگا

(1) :ماخذ کی شناخت، (2) مواد کی نسبت، (3) تاریخ اور وقت کی تصدیق، (4) عدمِ تحریف اور سالمیت، (5) حصول کے طریقے کی صحت، (6) تحویل و حفاظت کا ریکارڈ، (7) فنی و فرانزک جانچ، اور (8) دیگر شواہد سے مطابقت۔ یہ تمام امور اسلامی اصولِ تثبت، صدق، امانت اور عدمِ تحریف کے عمومی تقاضوں سے ہم آہنگ ہیں۔

اس بنا پر اسلامی قانونِ اثبات میں ڈیجیٹل شواہد کے استعمال کے لیے بنیادی اصول یہ ہوگا کہ ثبوت کی ڈیجیٹل صورت بذاتِ خود اس کی حجیت کا فیصلہ کن معیار نہیں، بلکہ اس کی حقیقت، نسبت، دلالت، صحت اور قابلِ اعتمادیت کی تحقیق اس کی اثباتی قدر متعین کرے گی۔ یوں جدید ڈیجیٹل وسائل کو اسلامی نظامِ اثبات کے بنیادی اصولوں کے ساتھ مربوط کرتے ہوئے ان کی فقہی تکییف شہادت، کتابت، اقرار یا قرینہ میں سے مناسب نوع کے مطابق کی جاسکتی ہے۔

پاکستانی قانون میں ڈیجیٹل شواہد

پاکستانی قانونی نظام میں ڈیجیٹل شواہد کی قانونی حیثیت کسی ایک قانون تک محدود نہیں بلکہ مختلف قوانین اور قانونی اصولوں کے مجموعی فریم ورک سے متعین ہوتی ہے۔ اس سلسلے میں **قانونِ شہادت آرڈر، 1984ء (Qanun-e-Shahadat Order, 1984)**، **Electronic Transactions Ordinance, 2002** اور **Prevention of Electronic Crimes Act, 2016** بنیادی اہمیت رکھتے ہیں۔ ان قوانین میں سے قانونِ شہادت کسی دعوے یا مقدمے میں پیش کیے جانے والے مواد کی شہادتی حیثیت سے متعلق بنیادی اصول فراہم کرتا ہے، Electronic Transactions Ordinance برقی دستاویزات، electronic communications اور electronic signatures کو قانونی ماحول فراہم کرتا ہے، جبکہ PECA 2016ء جرائمِ سائبر اور متعلقہ ڈیجیٹل معلومات کے حصول، تحفظ اور تفتیش کے قانونی پہلوؤں سے متعلق احکام فراہم کرتا ہے۔[27]

Electronic Transactions Ordinance, 2002ء اور ڈیجیٹل دستاویزات

Electronic Transactions Ordinance, 2002ء پاکستان میں برقی ذرائع سے ہونے والے معاملات اور electronic records کو قانونی نظام میں تسلیم کرنے کے لیے بنیادی قانون کی حیثیت رکھتا ہے۔ اس کا ایک اہم مقصد یہ ہے کہ کسی document، record، communication یا transaction کو صرف اس بنیاد پر قانونی اثر سے محروم نہ کیا جائے کہ وہ برقی

[27] Qanun-e-Shahadat Order, 1984؛ Electronic Transactions Ordinance, 2002؛ Prevention of Electronic Crimes Act, 2016.

یا electronic form میں ہے۔اس قانونی تصور نے تجارت، معاہدات، بینکاری، سرکاری معاملات اور دیگر قانونی سرگرمیوں میں electronic records کے استعمال کے لیے بنیادی قانونی بنیاد فراہم کی۔[28]

اس قانون میں electronic signatures اور electronic documents کے حوالے سے بھی اصول فراہم کیے گئے ہیں، جس کے نتیجے میں محض کسی دستاویز کے کاغذی صورت میں نہ ہونے کو اس کی قانونی حیثیت سے انکار کی کافی وجہ نہیں سمجھا جاتا۔تاہم کسی electronic record کا قانونی طور پر موجود ہونا اور کسی مخصوص مقدمے میں اس کی اصالت، نسبت اور اثباتی قدر ثابت ہونا دو الگ امور ہیں۔چنانچہ عدالت کے سامنے یہ سوال برقرار رہتا ہے کہ پیش کردہ record واقعی اسی ذریعے سے پیدا یا منتقل ہوا، جس سے اسے منسوب کیا جا رہا ہے، اور آیا اس کی سالمیت برقرار رہی یا نہیں۔

قانونِ شہادت آرڈر، 1984ء اور ڈیجیٹل شواہد

ڈیجیٹل شواہد کی عدالتی حیثیت میں Qanun-e-Shahadat Order, 1984 بنیادی اہمیت رکھتا ہے، کیونکہ عدالت کے سامنے پیش کیے جانے والے مواد کی relevance، proof اور evidentiary value کا جائزہ بالآخر قانونِ شہادت کے اصولوں کے تحت لیا جاتا ہے۔اگرچہ قانونِ شہادت بنیادی طور پر روایتی شہادتی تصورات کے ساتھ مرتب ہوا تھا، تاہم جدید ٹیکنالوجی کے استعمال اور بعد ازاں قانونی ترامیم نے electronic اور modern technological evidence کے لیے اس کے اندر اہم گنجائش پیدا کی ہے۔

اس ضمن میں آرٹیکل 164 خصوصی اہمیت رکھتا ہے۔اس میں عدالت کو اس امر کی گنجائش دی گئی ہے کہ وہ کسی معاملے کے ثبوت کے لیے ایسی evidence کو اجازت دے جو کسی جدید device یا technique کے ذریعے دستیاب ہوئی ہو۔[29] اس دفعہ کی اہمیت اس لیے بڑھ جاتی ہے کہ موجودہ دور میں mobile-phone data، audio/video recordings، CCTV footage، photographs، digital communications اور دیگر تکنیکی ذرائع سے حاصل ہونے والا مواد عدالتی تنازعات میں سامنے آ سکتا ہے۔

آرٹیکل 164 کا بنیادی قانونی تصور یہ ہے کہ جدید ٹیکنالوجی کے ذریعے حاصل ہونے والے شواہد کو محض اس بنیاد پر نظر انداز نہ کیا جائے کہ وہ روایتی طریقۂ شہادت سے مختلف ذریعے سے حاصل ہوئے ہیں۔تاہم اس کا یہ مطلب بھی نہیں کہ ہر digital output خود بخود قابلِ اعتماد یا فیصلہ کن ثبوت بن جاتا ہے۔عدالت کو متعلقہ evidence کی relevance، authenticity، integrity، source، attribution اور دیگر شواہد سے مطابقت کا جائزہ لینا ہوتا ہے۔

[28] Electronic Transactions Ordinance, 2002
[29] Qanun-e-Shahadat Order, 1984, art. 164.

آرٹیکل 73 اور بنیادی شہادت کا تصور

آرٹیکل 73 بنیادی شہادت (Primary Evidence) کے تصور سے متعلق ہے اور کسی دستاویز کے اصل وجود اور اس کی شہادتی پیش کش کے اصول کو بیان کرتا ہے۔ ڈیجیٹل ماحول میں اس دفعہ کا مطالعہ کرتے ہوئے روایتی مادی دستاویز اور electronic record کے درمیان فنی فرق کو ملحوظ رکھنا ضروری ہے۔ ڈیجیٹل فائل کی اصل، اس کی copy، اس کے electronic output اور اس سے تیار کردہ printout کے درمیان قانونی فرق بعض مقدمات میں اہم ہو سکتا ہے۔

اس لیے آرٹیکل 73 کو اس معنی میں نہیں لینا چاہیے کہ ہر electronic record محض electronic ہونے کی وجہ سے primary evidence قرار پاتا ہے یا ہر digital output خود بخود قابل قبول ہو جاتا ہے۔ بلکہ متعلقہ record کی نوعیت، اس کے اصل ماخذ، اس کے حصول کے طریقے اور قانون کے دیگر قابل اطلاق احکام کو سامنے رکھ کر اس کی شہادتی حیثیت متعین کی جائے گی۔ اسی طرح electronic evidence کے بارے میں دیگر متعلقہ قانونی دفعات اور عدالتی اصولوں کو بھی مجموعی طور پر ملحوظ رکھنا ضروری ہے۔

Prevention of Electronic Crimes Act, 2016 اور ڈیجیٹل شواہد

Prevention of Electronic Crimes Act, 2016 (PECA) پاکستان میں cyber offences اور ان سے متعلقہ electronic information کے لیے بنیادی خصوصی قانون ہے۔ اس قانون میں مختلف نوعیت کے سائبر جرائم، electronic information کی تفتیش اور متعلقہ قانونی کارروائی کے لیے فریم ورک فراہم کیا گیا ہے۔[30] اس اعتبار سے PECA کا تعلق محض "ڈیجیٹل ثبوت کی admissibility" سے نہیں بلکہ اس وسیع قانونی عمل سے ہے جس کے ذریعے کسی electronic device یا information system سے متعلق معلومات کو جرم کی تحقیق اور prosecution کے لیے حاصل، محفوظ اور استعمال کیا جا سکتا ہے۔

سائبر جرائم کے مقدمات میں mobile phones، computers، servers، social-media accounts، electronic communications، digital files اور دیگر electronic information تفتیش کا حصہ بن سکتی ہیں۔ تاہم کسی device سے data کا حاصل ہونا اور اس data کا عدالت میں کسی مخصوص شخص، وقت یا واقعے سے معتبر طور پر منسوب ہونا الگ الگ قانونی مسائل ہیں۔ اس لیے digital forensic examination، data preservation اور chain of custody جیسے امور عملی طور پر اہم ہو جاتے ہیں۔

قابل پیشی اور اثباتی قدر میں فرق

ڈیجیٹل شواہد کے قانونی تجزیے میں ایک بنیادی امتیاز قابل پیشی (admissibility) اور اثباتی قدر (probative value) کے درمیان ہے۔ کسی electronic record کو عدالت میں پیش کرنے کی اجازت مل جانا اس امر کے مترادف نہیں کہ

[30] Prevention of Electronic Crimes Act, 2016, especially the provisions relating to investigation, preservation and acquisition of information in relation to offences under the Act.

عدالت نے اس کے مندرجات کو قطعی طور پر درست تسلیم کر لیا ہے۔ اسی طرح کسی record کا بظاہر اصلی دکھائی دینا بھی اس کی نسبت اور سالمیت کو لازماً ثابت نہیں کرتا۔

عدالت کسی digital evidence کے بارے میں یہ سوالات اٹھا سکتی ہے کہ وہ کہاں سے حاصل ہوا؟ کس device یا system سے حاصل ہوا؟ کس شخص یا ادارے سے منسوب ہے؟ اس کی تحویل کس کے پاس رہی؟ کیا اس میں تبدیلی یا tampering کا امکان ہے؟ اس کے حصول اور preservation کا طریقہ کیا تھا؟ اور کیا دیگر آزاد شواہد اس کی تائید کرتے ہیں؟ ان سوالات کے جوابات اس evidence کی مجموعی اثباتی قدر کے تعین میں اہم کردار ادا کرتے ہیں۔

چنانچہ پاکستانی قانون کے تحت ڈیجیٹل شواہد کا تجزیہ محض electronic "ہونے" کی بنیاد پر نہیں کیا جا سکتا، بلکہ متعلقہ قانون، record کی نوعیت، اس کے ماخذ، نسبت، authenticity، integrity، طریقۂ حصول اور عدالتی scrutiny کو مجموعی طور پر سامنے رکھنا ضروری ہے۔ یوں پاکستانی قانونی نظام میں جدید ٹیکنالوجی سے حاصل ہونے والے شواہد کے لیے قانونی گنجائش موجود ہے، لیکن ان کی قبولیت اور اثباتی وزن کا حتمی تعین ہر مقدمے کے حقائق اور قابل اطلاق قانونی اصولوں کے مطابق کیا جائے گا۔

ڈیجیٹل شواہد کی Authentication اور Integrity

ڈیجیٹل شواہد کے عدالتی استعمال میں Authentication (اصالت و نسبت کی تصدیق) اور Integrity (سالمیت و عدمِ تحریف) بنیادی اہمیت رکھتے ہیں۔ ڈیجیٹل مواد کی محض موجودگی اس امر کو ثابت نہیں کرتی کہ وہ واقعی اسی شخص، device یا information system سے پیدا ہوا ہے جس کی طرف اسے منسوب کیا جا رہا ہے، اور نہ ہی یہ امر محض مشاہدے سے ثابت ہوتا ہے کہ حصول کے بعد اس میں کوئی تبدیلی نہیں کی گئی۔ اس لیے ڈیجیٹل شواہد کی اثباتی قدر متعین کرنے سے پہلے ان دونوں پہلوؤں کی تحقیق ضروری ہوتی ہے۔

Authentication سے مراد اس امر کی تصدیق ہے کہ پیش کیا جانے والا ڈیجیٹل مواد واقعی وہی ہے جس کے طور پر اسے عدالت کے سامنے پیش کیا جا رہا ہے اور وہ مناسب طور پر اپنے منسوب کردہ ماخذ سے مربوط ہے۔ مثلاً اگر کسی مقدمے میں WhatsApp message پیش کیا جائے تو یہ سوال اہم ہو گا کہ مذکورہ پیغام کس اکاؤنٹ، device یا system سے پیدا ہوا، آیا وہ اکاؤنٹ متعلقہ شخص کے زیرِ استعمال تھا، پیغام کے وقت device یا account تک رسائی کس کے پاس تھی، اور کیا دیگر تکنیکی شواہد اس نسبت کی تائید کرتے ہیں۔ اسی طرح کسی audio یا video recording کے بارے میں یہ تحقیق ضروری ہو سکتی ہے کہ recording کہاں اور کس device سے تیار ہوئی اور پیش کردہ فائل اصل record سے کس طرح حاصل کی گئی۔[31]

اس کے مقابلے میں Integrity سے مراد ڈیجیٹل ریکارڈ کی سالمیت ہے؛ یعنی اس بات کا اطمینان کہ ثبوت کے حصول، منتقلی، ذخیرے اور تجزیے کے دوران اس کے اصل data میں غیر مجاز یا غیر معلوم تبدیلی واقع نہیں ہوئی۔ ڈیجیٹل فائل کی copy بظاہر اصل فائل

[31] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. (Waltham, MA: Academic Press, 2011), 95–101.

سے یکساں ہو سکتی ہے، لیکن اس ظاہری یکسانیت سے خود بخود یہ ثابت نہیں ہوتا کہ data میں کوئی تبدیلی نہیں ہوئی۔ اسی لیے digital forensic examination میں ایسے فنی طریقے اختیار کیے جاتے ہیں جن کے ذریعے evidence کی حالت کو capture، document اور دوبارہ verify کیا جا سکے۔[32]

ڈیجیٹل فرانزک کے میدان میں Hash Value، Metadata، Forensic Imaging، Secure Acquisition اور دیگر تکنیکی طریقے evidence کی اصالت اور سالمیت کی جانچ میں معاون ہوتے ہیں۔ بالخصوص hash value کسی مخصوص digital file یا forensic image کی ایک فنی قدر فراہم کرتی ہے، جس کے ذریعے مختلف مراحل میں حاصل شدہ data کی مطابقت کو جانچا جا سکتا ہے۔ اسی طرح metadata میں file creation، modification، device اور دیگر تکنیکی معلومات شامل ہو سکتی ہیں، جو کسی digital record کے پس منظر اور زمانی ترتیب کو سمجھنے میں معاون ثابت ہوتی ہیں۔ تاہم کسی ایک technical indicator کو ہر صورت میں قطعی ثبوت قرار دینے کے بجائے اسے دیگر متعلقہ معلومات اور forensic findings کے ساتھ مجموعی طور پر دیکھنا زیادہ مناسب ہے۔[33]

Chain of Custody اور ڈیجیٹل شواہد

ڈیجیٹل شواہد کے تحفظ میں Chain of Custody ایک اہم فنی و قانونی تصور ہے۔ اس سے مراد evidence کی تحویل اور نقل و انتقال کا ایسا مسلسل اور دستاویزی ریکارڈ ہے جس سے یہ معلوم ہو سکے کہ ثبوت کس شخص یا ادارے نے، کس وقت، کس مقام پر، کس طریقے سے حاصل کیا، کس حالت میں محفوظ کیا، کس کے حوالے کیا اور بعد میں اس پر کیا کارروائی کی گئی۔ اس کا مقصد یہ دکھانا ہوتا ہے کہ evidence کے حصول سے لے کر عدالت میں پیش کیے جانے تک اس کے ساتھ ہونے والی کارروائی قابلِ تعین اور قابلِ جانچ رہی، اور اس میں غیر مجاز تبدیلی یا tampering کے امکان کو مناسب حد تک کنٹرول کیا گیا۔[34]

خصوصاً mobile phone، computer، hard drive، USB، server یا دیگر digital storage device سے evidence حاصل کرتے وقت اصل device اور اس سے حاصل کیے گئے forensic image یا data کے درمیان تعلق کو مناسب طور پر document کرنا ضروری ہوتا ہے۔ اگر evidence کے حصول اور preservation کے مراحل واضح نہ ہوں تو عدالت کے لیے یہ جانچنا مشکل ہو سکتا ہے کہ پیش کردہ مواد وہی ہے جو اصل device یا system سے حاصل کیا گیا تھا اور اس دوران اس کی حالت میں کوئی غیر مجاز تبدیلی واقع ہوئی یا نہیں۔

---

[32] Karen Kent et al., Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86

[33] National Institute of Standards and Technology, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Revision 1 (Gaithersburg, MD: NIST, 2014), 1–6.

[34] International Organization for Standardization, ISO/IEC 27037:2012: Information Technology—Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence (Geneva: ISO, 2012), 1–4.

Authenticationاور Integrity کی باہمی نسبت

Authenticationاور Integrity ایک دوسرے سے مربوط ضرور ہیں، لیکن دونوں ایک ہی مفہوم نہیں رکھتے۔ Authenticationبنیادی طور پر ماخذ، نسبت اور شناخت کے سوال سے متعلق ہے، جبکہ Integrity مواد کی سالمیت اور عدم تحریف سے متعلق ہے۔ ممکن ہے کوئی فائل بظاہر مکمل طور پر محفوظ اور unchanged ہو، لیکن اس کی اصل نسبت ہی ثابت نہ ہو؛ اسی طرح کسی recordکا ماخذ معلوم ہو سکتا ہے لیکن اگر اس کی سالمیت مشکوک ہو تو اس کے موجودہ مندرجات کی اثباتی قدر متاثر ہو سکتی ہے۔ اس لیے قابلِ اعتماد ڈیجیٹل evidence کے لیے دونوں پہلوؤں کا الگ الگ جائزہ ضروری ہے۔

اسلامی اصولِ امانت اور ڈیجیٹل شواہد

ڈیجیٹل شواہد کے تحفظ اور ان کی تحویل کے اس فنی تصور میں اسلامی اصولِ **امانت** سے ایک اصولی مناسبت پائی جاتی ہے۔ قرآن مجید میں اللہ تعالیٰ کا ارشاد ہے:

إِنَّ اللهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَىٰ أَهْلِهَا[35] بے شک اللہ تمہیں حکم دیتا ہے کہ امانتیں ان کے حق داروں تک پہنچاؤ۔

اگرچہ آیتِ کریمہ کا مفہوم اس مخصوص جدید فنی اصطلاح تک محدود نہیں، تاہم اصولی اعتبار سے یہ ہدایت اس امر کی اہمیت واضح کرتی ہے کہ کسی کے سپرد کی گئی چیز یا معلومات میں خیانت، تحریف یا غیر مجاز تصرف نہ کیا جائے۔ اسی عمومی اصول کی روشنی میں ڈیجیٹل شواہد کے معاملے میں بھی evidence کی صحیح حفاظت، اس کے اصل مواد میں غیر مجاز تبدیلی سے اجتناب، اس کی تحویل کے مراحل کی درست دستاویز بندی اور عدالت کے سامنے اسے امانت و دیانت کے ساتھ پیش کرنا اہم تقاضے قرار پاتے ہیں۔

اس طرحAuthentication، Integrityاور Chain of Custody صرف تکنیکی اصطلاحات نہیں بلکہ ڈیجیٹل شواہد کی قابلِ اعتمادیت کے بنیادی اجزاء ہیں۔ کسی digital evidence کی شرعی یا قانونی اثباتی قدر متعین کرتے وقت اس کے ماخذ، نسبت، سالمیت، حصول کے طریقے اور تحویل کے تسلسل کی مناسب تحقیق اس لیے ضروری ہے کہ عدالت کے سامنے پیش کیا جانے والا مواد قابلِ اعتماد اور قابلِ جانچ بنیاد پر قائم ہو۔

ڈیجیٹل شواہد اور پرائیویسی

ڈیجیٹل شواہد کے حصول، تحفظ اور عدالتی استعمال میں شخصی رازداری (Privacy) اور انسانی حرمت کا مسئلہ خصوصی اہمیت رکھتا ہے۔ جدید ڈیجیٹل آلات، بالخصوص موبائل فون، کمپیوٹر اور آن لائن اکاؤنٹس، کسی شخص کی نجی زندگی سے متعلق وسیع نوعیت کی معلومات محفوظ رکھتے ہیں، جن میں ذاتی گفتگو، تصاویر، ویڈیوز، رابطہ معلومات، مالی معاملات، location data، browsing historyاور دیگر نجی معلومات شامل ہو سکتی ہیں۔ اس لیے کسی digital device یا account سے معلومات حاصل کرنا محض ایک تکنیکی کارروائی نہیں بلکہ بعض صورتوں میں براہِ راست شخصی زندگی اور نجی دائرے میں مداخلت کا باعث بن سکتا ہے۔

---

[35] القرآن الکریم، النساء 4: 58۔

اسلامی شریعت نے انسانی عزت، شخصی حرمت اور نجی زندگی کے تحفظ کو بنیادی اخلاقی و معاشرتی اصولوں میں شمار کیا ہے۔ قرآن مجید میں واضح طور پر ارشاد فرمایا گیا:

وَلَا تَجَسَّسُوا[36] اور تجسس نہ کرو۔

اسی طرح سورۂ نور میں دوسروں کے گھروں میں داخل ہونے کے لیے اجازت طلب کرنے کا حکم بھی شخصی حرمت اور نجی دائرے کے احترام کی اہمیت کو ظاہر کرتا ہے۔

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ۚ ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ[37] اے ایمان والو! اپنے گھروں کے علاوہ دوسرے گھروں میں داخل نہ ہوا کرو، یہاں تک کہ اجازت لے لو اور ان کے رہنے والوں کو سلام کر لو۔ یہ تمہارے لیے بہتر ہے، تاکہ تم نصیحت حاصل کرو۔

ان نصوص سے یہ اصول سامنے آتا ہے کہ کسی شخص کی نجی معلومات تک بلاجواز رسائی، ان کی تلاش، نگرانی یا افشا کو محض معلومات حاصل کرنے کی خواہش کی بنیاد پر جائز قرار نہیں دیا جا سکتا۔

اسی بنا پر کسی مقدمے میں digital evidence کی ممکنہ اہمیت بذاتِ خود اس امر کا جواز نہیں بنتی کہ کسی شخص کے موبائل فون، نجی اکاؤنٹ، ذاتی پیغامات یا دیگر private data تک ہر صورت میں رسائی حاصل کر لی جائے۔ ثبوت کے حصول کا قانونی جواز، متعلقہ شخص کی رازداری، ضرورت، تناسب اور حصول کے مجاز طریقے کو ملحوظ رکھنا ضروری ہے۔ خصوصاً سرکاری یا تفتیشی اداروں کی جانب سے کسی device یا account سے data حاصل کرتے وقت یہ سوال اہم ہو جاتا ہے کہ آیا اس کے لیے مناسب قانونی اختیار موجود تھا، کیا حاصل کیا جانے والا data متعلقہ مقدمے سے واقعی متعلق تھا، اور کیا مطلوبہ مقصد حاصل کرنے کے لیے اتنی ہی مداخلت ضروری تھی۔

پاکستانی قانونی تناظر میں بھی آئینِ پاکستان کا آرٹیکل 14 انسان کی dignity اور گھر کی privacy کو تحفظ فراہم کرتا ہے۔[38] اگرچہ digital privacy کے تمام جدید مسائل کو صرف ایک آئینی شق سے حل نہیں کیا جا سکتا، تاہم شخصی وقار اور نجی زندگی کا یہ آئینی تحفظ اس امر کی بنیاد فراہم کرتا ہے کہ ریاستی یا قانونی کارروائی کے دوران شہری کی نجی معلومات کے ساتھ من مانی مداخلت نہ کی جائے۔

ڈیجیٹل شواہد کے باب میں ضرورت اور تناسب (necessity and proportionality) کا اصول خصوصی اہمیت رکھتا ہے۔ اگر کسی مقدمے کے لیے کسی مخصوص پیغام، فائل یا transaction record کی ضرورت ہو تو غیر متعلقہ شخصی معلومات کے پورے ذخیرے تک بلاضرورت رسائی یا اسے عام کرنا رازداری کے تحفظ کے اصول سے متصادم ہو سکتا ہے۔ اسی طرح اگر کسی device سے قانونی طریقے سے evidence حاصل کیا گیا ہو تو اس device میں موجود تمام نجی معلومات کو بلاضرورت مقدمے کے علاوہ دیگر مقاصد کے لیے استعمال یا افشا کرنا بھی الگ قانونی و اخلاقی سوال پیدا کر سکتا ہے۔

---

[36] القرآن الکریم، الحجرات 49: 12۔

[37] القرآن الکریم، النور 24: 27۔

[38] Constitution of the Islamic Republic of Pakistan, 1973, art. 14(1)

یہاں ثبوت کے حصول اور ثبوت کے افشا میں بھی فرق کرنا ضروری ہے۔ کسی مخصوص قانونی مقصد کے لیے عدالت یا مجاز تفتیشی ادارے کے ذریعے کسی digital record کا حصول ایک الگ مرحلہ ہے، جبکہ اس record کو غیر متعلقہ افراد تک پہنچانا، عوامی سطح پر نشر کرنا یا مقدمے کی ضرورت سے زائد استعمال کرنا الگ معاملہ ہے۔ چنانچہ ڈیجیٹل evidence کی حفاظت میں confidentiality اور access control بھی اہم تقاضے بن جاتے ہیں۔

اسلامی اصولوں کی روشنی میں اس معاملے میں دو بنیادی تقاضوں کے درمیان توازن ضروری ہے: ایک طرف حقوق کے تحفظ، ظلم کے ازالے اور جرائم کی تحقیق کے لیے ضروری شواہد کا حصول، اور دوسری طرف بلا جواز تجسس، شخصی حرمت کی پامالی اور نجی معلومات کے غیر ضروری افشا سے اجتناب۔ ان دونوں میں سے کسی ایک کو بالکل نظر انداز کرنا متوازن نظامِ اثبات کے تقاضوں سے ہم آہنگ نہیں ہوگا۔

لہٰذا ڈیجیٹل شواہد کے حصول اور استعمال کے لیے اصولی طور پر یہ تقاضے سامنے آتے ہیں کہ قانونی اختیار موجود ہو، مقصد جائز اور متعلقہ ہو، حصول ضرورت کے مطابق محدود ہو، غیر متعلقہ نجی معلومات کو حتی الامکان محفوظ رکھا جائے، evidence تک رسائی مجاز افراد تک محدود ہو، اور اسے صرف قانونی و متعلقہ مقصد کے لیے استعمال کیا جائے۔ اس طرح ڈیجیٹل شواہد کے ذریعے حقوق اور انصاف کے تحفظ کے ساتھ ساتھ انسانی وقار اور شخصی رازداری کے تقاضوں کو بھی برقرار رکھا جا سکتا ہے۔

مقدمہ: ظہیر احمد خان بنام حکومت سندھ و دیگر[39]

ا۔ مقدمے کے حقائق

درخواست گزار ظہیر احمد خان نے آئینِ پاکستان کے آرٹیکل 199 کے تحت سندھ ہائی کورٹ سے رجوع کیا۔ معاملہ یہ تھا کہ ماتحت عدالت نے درخواست گزار کی اس درخواست کو مسترد کر دیا تھا جس میں اس نے اپنے گواہوں کا بیانِ اوّل حلف نامے کے ذریعے ریکارڈ کروانے کی اجازت طلب کی تھی۔ ماتحت عدالت کا مؤقف تھا کہ گواہوں کو کھلی عدالت میں حاضر ہو کر اپنا بیان ریکارڈ کروانا چاہیے اور درخواست گزار نے یہ ثابت نہیں کیا کہ گواہوں کو عدالت میں پیش کرنے کے بجائے حلف نامے کے ذریعے ان کا بیان لینے کی کوئی معقول وجہ موجود ہے۔ درخواست گزار نے اس حکم کے خلاف نظرِ ثانی کی درخواست دائر کی، تاہم ضلعی عدالت میرپور خاص نے بھی ماتحت عدالت کا حکم برقرار رکھا۔

بعد ازاں درخواست گزار نے سندھ ہائی کورٹ سے رجوع کرتے ہوئے مؤقف اختیار کیا کہ قانون میں ایسی مطلق ممانعت موجود نہیں کہ ہر صورت میں گواہ کی شہادت صرف عدالت میں جسمانی حاضری کے ذریعے ہی ریکارڈ کی جائے۔ اس نے ضابطۂ دیوانی کے متعلقہ احکام اور قانونِ شہادت کے متعلقہ آرٹیکلز کی بنیاد پر حلف نامے کے ذریعے بیانِ شہادت پیش کرنے کی اجازت طلب کی۔

[39] Zaheer Ahmed Khan v. Government of Sindh & others, Constitution Petition No. D-30 of 2024, Sindh High Court, Circuit Court Mirpurkhas, Order dated 19.08.2024.

۲۔ قانونی سوال

اس مقدمے میں بنیادی سوال یہ تھا کہ: کیا عدالت مناسب حالات میں جدید آلات اور تکنیک کے ذریعے گواہ کی شہادت ریکارڈ کرنے کی اجازت دے سکتی ہے، اور کیا قانونِ شہادت آرڈر 1984ء کا آرٹیکل 164 ایسی جدید تکنیک کے ذریعے دستیاب ہونے والی شہادت کو عدالت میں پیش کرنے کی اجازت دیتا ہے؟

اس کے ساتھ یہ سوال بھی زیرِ غور آیا کہ آیا گواہ کا عدالت میں جسمانی طور پر موجود ہونا ہر حال میں ضروری ہے، یا مناسب حالات میں ویڈیو کانفرنسنگ کے ذریعے مجازی حاضری اختیار کرتے ہوئے بھی اس کی شہادت ریکارڈ کی جاسکتی ہے۔

۳۔ آرٹیکل 164 کی قانونی حیثیت

فاضل عدالت نے قانونِ شہادت آرڈر 1984ء کے آرٹیکل 164 کو صراحت کے ساتھ زیرِ بحث لاتے ہوئے اس کا مفہوم بیان کیا کہ:

ایسے مقدمات میں جنہیں عدالت مناسب سمجھے، جدید آلات یا تکنیک کے ذریعے دستیاب ہونے والی کسی بھی شہادت کو عدالت میں پیش کرنے کی اجازت دی جاسکتی ہے۔ اس شق کا بنیادی مقصد یہ ہے کہ شہادت کے حصول اور پیش کرنے کے طریقہ کار کو جدید تکنیکی ترقی کے باعث پیدا ہونے والے نئے ذرائع تک محدود نہ رکھا جائے۔

۴۔ عدالت کی تشریح

فاضل سندھ ہائی کورٹ نے سپریم کورٹ کے طے شدہ اصول کی روشنی میں قرار دیا کہ ضابطۂ دیوانی کے آرڈر XVIII رول 4 میں استعمال ہونے والی گواہ کی حاضری کو موجودہ تکنیکی دور کے تناظر میں مجازی حاضری تک وسعت دی جاسکتی ہے۔ چنانچہ مناسب حالات میں گواہ ویڈیو کانفرنسنگ کے ذریعے بھی عدالت کے سامنے اپنا بیان ریکارڈ کرا سکتا ہے، بشرطیکہ عدالت اس بات کو یقینی بنائے کہ گواہ آزادانہ طور پر بیان دے رہا ہے اور کسی بیرونی دباؤ یا غیر مناسب اثر کے تحت نہیں ہے۔

عدالت نے واضح کیا کہ قانونِ شہادت آرڈر 1984ء کا آرٹیکل 164 جدید آلات اور تکنیک کے ذریعے دستیاب ہونے والی شہادت کو عدالت میں پیش کرنے کی قانونی گنجائش فراہم کرتا ہے۔ اس میں ویڈیو کانفرنسنگ کے ذریعے دستیاب ہونے والی گواہ کی زبانی شہادت بھی شامل ہو سکتی ہے۔

فاضل عدالت کے مطابق جدید ٹیکنالوجی کے استعمال سے انصاف تک رسائی میں سہولت پیدا ہوتی ہے، مقدمات کے فیصلے میں غیر ضروری تاخیر اور اخراجات کم ہو سکتے ہیں اور انصاف کی فراہمی کو زیادہ مؤثر بنایا جاسکتا ہے۔ اس تناظر میں عدالت نے آئینِ پاکستان کے آرٹیکلز 9 اور 10 A- اور اصولِ پالیسی کے آرٹیکل 37 د (کے تقاضوں کو بھی پیشِ نظر رکھا۔

۵۔ حلف نامے کے ذریعے شہادت

عدالت نے یہ بھی قرار دیا کہ حلف نامے کے ذریعے شہادت پیش کرنے کو ہر حال میں ناقابلِ قبول قرار نہیں دیا جاسکتا۔ عدالت کو ضابطۂ دیوانی کی دفعہ 151 کے تحت مناسب حالات میں اپنی صوابدید استعمال کرنے کا اختیار حاصل ہے۔ تاہم حلف نامے کے ذریعے پیش کی جانے والی شہادت دوسرے فریق کے حقِ جرح کے تابع ہو گی۔ اگر مخالف فریق حلف نامے میں موجود بیان کو چیلنج کرے یا حلف نامہ دینے والے شخص سے

جرح کا مطالبہ کرے تو متعلقہ شخص کو جرح کے لیے پیش کرنا ضروری ہوگا۔ اگر اسے جرح کے لیے پیش نہ کیا جائے تو اس حلف نامے پر بطور شہادت انحصار نہیں کیا جاسکے گا۔ اس اصول کی بنیاد منصفانہ سماعت، قدرتی انصاف اور حقِ جرح پر ہے۔

۶۔ عدالت کا فیصلہ

سندھ ہائی کورٹ نے قرار دیا کہ ماتحت عدالت اور نظرثانی کی عدالت نے درخواست گزار کی درخواست مسترد کرتے ہوئے مناسب قانونی صوابدید استعمال نہیں کی۔

فاضل عدالت کے نزدیک گواہوں کو مناسب شرائط کے ساتھ حلف نامے کی صورت میں اپنا بیانِ اوّل پیش کرنے کی اجازت دی جاسکتی تھی، کیونکہ مخالف فریق کو بعد ازاں ان گواہوں پر جرح کا مکمل حق حاصل تھا۔

چنانچہ سندھ ہائی کورٹ نے ماتحت عدالت اور نظرثانی کی عدالت کے دونوں احکامات کو کالعدم قرار دیتے ہوئے درخواست منظور کرلی اور درخواست گزار کو اپنے گواہوں کا بیانِ اوّل حلف نامۂ شہادت کی صورت میں پیش کرنے کی اجازت دی، تاہم اسے دوسرے فریق کے حقِ جرح سے مشروط رکھا۔ عدالت نے مقدمے کی کارروائی دو ماہ کے اندر مکمل کرنے کی بھی ہدایت کی۔

۷۔ حاصل شدہ قانونی اصول

اس فیصلے سے آرٹیکل 164 کے حوالے سے یہ اصول سامنے آتا ہے کہ: قانونِ شہادت آرڈر 1984ء کا آرٹیکل 164 جدید آلات اور تکنیک کے ذریعے دستیاب ہونے والی شہادت کو عدالت میں پیش کرنے کی اجازت دیتا ہے۔ جدید تکنیکی ذریعہ استعمال ہونے کی وجہ سے کوئی شہادت محض اسی بنیاد پر ناقابلِ قبول نہیں ہوجاتی، بلکہ عدالت اس کے استعمال کی مناسبت، قابلِ اعتمادیت، منصفانہ سماعت اور فریقین کے حقِ جرح کو ملحوظ رکھتے ہوئے فیصلہ کرتی ہے۔

خصوصاً ویڈیو کانفرنسنگ کے ذریعے گواہ کی مجازی حاضری کو جدید تکنیک کے ذریعے دستیاب ہونے والی شہادت کے طور پر آرٹیکل 164 کے دائرۂ کار میں تسلیم کیا گیا ہے۔

اس سے واضح ہوتا ہے کہ پاکستانی قانون شہادت میں جدید ٹیکنالوجی سے حاصل ہونے والی شہادت کے لیے قانونی گنجائش موجود ہے۔

یہ فیصلہ اس امر کی تائید کرتا ہے کہ شہادت کا جدید یا ڈیجیٹل ذریعہ بذاتِ خود اسے ناقابلِ قبول نہیں بناتا، بلکہ عدالت اس کے قانونی استعمال، طریقۂ حصول، قابلِ اعتمادیت اور فریقین کے بنیادی حقوق کو سامنے رکھ کر اس کے بارے میں فیصلہ کرسکتی ہے۔

شریعت اور پاکستانی قانون کا تقابلی تجزیہ

اسلامی قانونِ اثبات اور پاکستانی قانونی نظام کا ڈیجیٹل شواہد کے حوالے سے تقابلی مطالعہ یہ ظاہر کرتا ہے کہ دونوں نظاموں میں بعض بنیادی اصولی سطحوں پر قابلِ ذکر موافقت پائی جاتی ہے، اگرچہ ان اصولوں کی قانونی و فقہی تعبیر اور عملی تطبیق میں فرق موجود ہے۔ دونوں نظاموں میں ثبوت کو محض اس کی ظاہری شکل کی بنیاد پر قبول کرنے کے بجائے اس کے ماخذ، نسبت، صداقت اور متعلقہ واقعے سے تعلق کو اہمیت دی جاتی ہے۔

سب سے پہلی مماثلت تحقیق خبر اور ثبوت کی تصدیق کے اصول میں ہے۔ اسلامی شریعت نے خبر کے معاملے میں تحقیق، تثبت اور تبین کی تاکید کی ہے۔ قرآن مجید کا ارشاد ہے: ﴿فَتَبَيَّنُوا﴾[40] یعنی "تحقیق کر لیا کرو۔" اس کے مقابلے میں جدید قانونی نظام میں بھی کسی digital evidence کی authenticity، integrity اور reliability کا جائزہ اس لیے لیا جاتا ہے کہ عدالت کے سامنے پیش کیا جانے والا مواد قابلِ اعتماد بنیاد پر قائم ہو۔ اس اعتبار سے دونوں نظاموں میں ثبوت کی صحت اور قابلِ اعتمادیت کی تحقیق ایک مشترک بنیادی مقصد کے طور پر سامنے آتی ہے۔

دوسری مماثلت حقوق کے تحفظ اور عدل کے قیام میں ہے۔ اسلامی شریعت میں عدل، حق کی ادائیگی اور ظلم سے اجتناب بنیادی قانونی و اخلاقی مقاصد میں شامل ہیں۔ قرآن مجید میں عدل کے قیام کا حکم دیا گیا ہے: ﴿إِنَّ اللهَ يَأْمُرُ بِالْعَدْلِ وَالْإِحْسَانِ﴾۔[41] اسی طرح عدالتی نظام میں evidence کا بنیادی عملی مقصد عدالت کو متعلقہ واقعات اور تنازع کے حقائق کے تعین میں مدد فراہم کرنا ہے، تاکہ قانونی فیصلہ قابلِ اعتماد شہادتی مواد کی بنیاد پر کیا جا سکے۔

تیسری مماثلت قرائن اور circumstantial evidence کے استعمال میں دیکھی جا سکتی ہے۔ اسلامی فقہ میں بعض حالات میں خارجی علامات اور قرائن کے ذریعے کسی پوشیدہ حقیقت تک استدلالی رسائی کی گنجائش موجود ہے۔ ابن القیم نے قضائی معاملات میں قرائن اور حالات کی اہمیت پر تفصیلی بحث کی ہے۔ جدید قانونی نظام میں بھی circumstantial evidence کو اس کی متعلقیت، اعتماد اور مقدمے کے دیگر شواہد کے ساتھ تعلق کی بنیاد پر زیرِ غور لایا جاتا ہے۔ ڈیجیٹل ماحول میں CCTV footage، GPS data، call records، access logs اور بعض metadata اسی نوع کے شواہد کے طور پر سامنے آ سکتے ہیں۔

چوتھی مماثلت تحریف، جعل سازی اور جھوٹی معلومات سے اجتناب کے اصول میں ہے۔ اسلامی شریعت نے جھوٹی گواہی اور قولِ زور کی شدید مذمت کی ہے۔ رسول اللہ ﷺ نے فرمایا: أَلَا وَقَوْلُ الزُّورِ،[42] اور آپ ﷺ نے اس تنبیہ کو بار بار بیان فرمایا۔ جدید digital forensics میں بھی evidence کی integrity، preservation اور chain of custody پر اس لیے توجہ دی جاتی ہے کہ record میں غیر مجاز تبدیلی، tampering یا manipulation کو شناخت اور روکنے کی کوشش کی جا سکے۔

اس کے باوجود دونوں نظاموں کے درمیان اصولی و تفصیلی اختلافات بھی موجود ہیں۔ پاکستانی قانون میں کسی digital evidence کی admissibility، اس کے حصول کا طریقۂ کار، اس کی قانونی relevance اور اس کی evidentiary weight کا تعین متعلقہ قانونی دفعات، قواعدِ شہادت اور عدالتی تشریحات کے ذریعے ہوتا ہے۔ اس کے برعکس اسلامی فقہ میں کسی ثبوت کی حجیت کا تعین اس کی فقہی تکییف، متعلقہ نصوص، اصولِ فقہ اور بابِ قضاء و شہادات کے مقررہ شرعی معیار کی روشنی میں کیا جاتا ہے۔

یہ فرق خاص طور پر ان مقدمات میں نمایاں ہو جاتا ہے جہاں شریعت نے اثبات کا مخصوص اور متعین معیار مقرر کیا ہو۔ مثلاً حدود کے بعض جرائم میں شرعی نصوص نے اثبات کے لیے مخصوص شرائط مقرر کی ہیں۔ ایسے معاملات میں کسی digital record کا تکنیکی طور پر

---

[40] القرآن الکریم، الحجرات 49: 6۔

[41] القرآن الکریم، النحل 16: 90

[42] محمد بن إسماعيل البخاري، صحيح البخاري، كتاب الشهادات، باب ماقيل في شهادة الزور، حديث رقم 2654

authenticاور reliable ہونا اپنی جگہ اہم ہو سکتا ہے، لیکن محض اس بنیاد پر اسے ہر قسم کے شرعی دعوے کے لیے اس مقررہ معیارِ اثبات کا قائم مقام قرار نہیں دیا جا سکتا۔ دوسرے لفظوں میں technical authenticityاور شرعی حجیت ایک ہی مفہوم نہیں ہیں۔ اسی طرح کسی digital evidence کی قانونی admissibility اور اس کی حتمی اثباتی قدر کو بھی ایک دوسرے سے الگ رکھنا ضروری ہے۔ ایک record قانونی طور پر عدالت کے سامنے پیش کیا جا سکتا ہے، لیکن اس کی نسبت، سالمیت، دلالت اور دیگر شواہد کے ساتھ مطابقت کے جائزے کے بعد ہی اس کے evidentiary weight کا تعین ہو گا۔ اسی طرح شرعی تناظر میں بھی کسی digital materialکی موجودگی اور اس کی فقہی حجیت کے درمیان فرق ملحوظ رکھنا ضروری ہے۔

تقابلی مطالعے سے یہ بھی واضح ہوتا ہے کہ ڈیجیٹل شواہد کی فنی نوعیت بذاتِ خود نہ تو اسے شرعی شہادت بناتی ہے اور نہ ہی ہر صورت میں فیصلہ کن قانونی ثبوت۔ اس کی حیثیت اس کے ماخذ، نسبت، دلالت، اصالت، سالمیت، حصول کے طریقے اور متعلقہ مقدمے کے قانونی یا شرعی معیار کے مطابق متعین ہو گی۔ چنانچہ ایک ہی digital record مختلف قانونی و شرعی سیاق میں مختلف اثباتی حیثیت رکھ سکتا ہے۔

لہٰذا تحقیقی طور پر زیادہ محتاط نتیجہ یہ ہے کہ ڈیجیٹل شواہد کے عمومی اصولوں، بالخصوص تحقیق، تصدیق، سالمیت، حقوق کے تحفظ اور معتبر قرائن سے استدلال کے میدان میں اسلامی قانونِ اثبات اور پاکستانی قانونی نظام کے درمیان اصولی موافقت پائی جاتی ہے؛ تاہم مخصوص مقدمات میں اس کی حجیت اور اثباتی قوت کا تعین متعلقہ شرعی اور قانونی معیار کے مطابق الگ الگ کیا جائے گا۔ اس لیے جدید ڈیجیٹل وسائل کو اسلامی قانونِ اثبات کے ساتھ مربوط کرتے ہوئے نہ تو ہر digital record کو بلا تفریق شرعی دلیل قرار دینا مناسب ہے اور نہ ہی اس کی فنی حیثیت کو نظر انداز کرنا؛ بلکہ دونوں نظاموں کے اپنے اپنے معیار کو برقرار رکھتے ہوئے ان کے درمیان علمی تطبیق پیدا کرنا زیادہ مناسب تحقیقی منہج ہو گا۔

نتائج

- ڈیجیٹل انقلاب نے نظامِ اثبات کی روایتی ساخت کو نمایاں طور پر تبدیل کر دیا ہے۔ موجودہ دور میں عدالت کے سامنے پیش ہونے والا ثبوت صرف انسانی شہادت، تحریری دستاویز یا مادی شے تک محدود نہیں رہا، بلکہ موبائل فون، کمپیوٹر، سرور، CCTV، GPS، برقی مراسلات، سماجی رابطوں کے ذرائع، کال ڈیٹیل ریکارڈ، میٹا ڈیٹا اور دیگر ڈیجیٹل ذرائع بھی واقعات اور حقائق کے تعین میں اہم کردار ادا کر رہے ہیں۔ اس صورتِ حال نے ایک طرف جدید ذرائعِ اثبات سے استفادے کے نئے امکانات پیدا کیے ہیں اور دوسری طرف ثبوت کی نسبت، صحت، سالمیت اور قابلِ اعتماد ہونے سے متعلق نئے فقہی و قانونی سوالات بھی پیدا کیے ہیں۔
- اسلامی شریعت کے اصولی مطالعے سے واضح ہوتا ہے کہ کسی ثبوت کی حجیت محض اس کی ظاہری شکل یا مادی صورت پر منحصر نہیں، بلکہ اس کے صدق، تحقیق، دلالت، نسبت، امانت اور حقائق سے مطابقت بنیادی اہمیت رکھتی ہے۔ قرآن و سنت اور فقہی اصولوں کی روشنی میں ڈیجیٹل مواد کو اس کی حقیقی اثباتی نوعیت کے مطابق مختلف فقہی قالبوں میں تکییف کیا جا سکتا ہے۔ چنانچہ مستند ڈیجیٹل تحریر اور برقی دستاویز کتابت، معتبر طور پر منسوب ڈیجیٹل اعترافِ اقرار، براہِ راست انسانی بیان کے لیے استعمال ہونے والا ڈیجیٹل ذریعہ شہادت کی ادائیگی کا وسیلہ، جبکہ CCTV، GPS، کال ریکارڈ، سرور لاگز اور دیگر خودکار تکنیکی معلومات عموماً قرائن کے طور پر تکییف کی جا

سکتی ہیں۔اس سے یہ اصول سامنے آتا ہے کہ ڈیجیٹل ہونے کی حیثیت بذاتِ خود کسی ثبوت کی شرعی نوعیت متعین نہیں کرتی، بلکہ اس کا حقیقی اثباتی کردار بنیادی معیار ہے۔

- پاکستانی قانون کے مطالعے سے بھی معلوم ہوتا ہے کہ جدید تکنیکی ذرائع کو نظامِ اثبات سے خارج نہیں کیا گیا، بلکہ قانونِ شہادت آرڈر 1984ء کے متعلقہ احکام، خصوصاً آرٹیکل 164، اور الیکٹرانک ٹرانزیکشنز آرڈیننس 2002ء سمیت دیگر متعلقہ قوانین نے برقی اور تکنیکی معلومات کے قانونی استعمال کے لیے بنیاد فراہم کی ہے۔تاہم کسی ڈیجیٹل مواد کا محض دستیاب یا قابلِ پیش کش ہونا اس کی حتمی اثباتی قدر کو ثابت نہیں کرتا۔اس کی Authentication، Integrity، Chain of Custody اور ضرورت کے مطابق Forensic Verification اس امر کے تعین میں اہم کردار ادا کرتی ہیں کہ پیش کردہ مواد واقعی اسی ماخذ سے متعلق ہے جس کی طرف اسے منسوب کیا جا رہا ہے اور حصول و حفاظت کے مراحل میں اس میں کوئی غیر مجاز تبدیلی نہیں ہوئی۔
- فقہی اور قانونی دونوں زاویوں سے یہ امتیاز بھی ملحوظ رہنا ضروری ہے کہ قابلِ قبول ہونا اور قطعی طور پر ثابت کر دینا ایک ہی امر نہیں۔ کوئی ڈیجیٹل مواد قانونی طور پر قابلِ سماعت یا فقہی اعتبار سے قابلِ التفات ہو سکتا ہے، لیکن اس کی اثباتی قوت کا تعین اس کی نوعیت، دلالت، نسبت، صحت، سالمیت، مقدمے کے حالات اور دیگر مؤید شواہد کی روشنی میں کیا جائے گا۔اسی طرح ایسے معاملات جن میں شریعت نے اثبات کے لیے مخصوص نصاب یا خاص طریقۂ اثبات مقرر کیا ہے، وہاں کسی ڈیجیٹل ریکارڈ کی فنی صحت کو بلا تحقیق اس مخصوص شرعی معیار کا قائم مقام قرار نہیں دیا جا سکتا۔
- لہٰذا اس پورے مطالعے کا جامع نتیجہ یہ ہے کہ ڈیجیٹل شواہد نہ بذاتِ خود ناقابلِ قبول ہیں اور نہ ہر صورت میں قطعی حجت؛ ان کی شرعی و قانونی حیثیت ان کی حقیقی نوعیت، متعلقیت، ماخذ و نسبت، صداقت، سالمیت، حصول و حفاظت کے طریقۂ کار اور متعلقہ مقدمے کے شرعی و قانونی معیارِ اثبات کی بنیاد پر متعین ہو گی۔ چنانچہ جدید ڈیجیٹل ذرائع سے استفادہ کرتے ہوئے ایک ایسا متوازن منہج اختیار کرنا ضروری ہے جو ایک طرف ٹیکنالوجی کے فراہم کردہ معتبر ذرائعِ معلومات اور قرائن سے فائدہ اٹھائے اور دوسری طرف تحقیق، احتیاط، حقوقِ افراد، عدل اور شرعی اصولِ اثبات کو ملحوظ رکھے۔ یہی طرزِ عمل جدید نظامِ اثبات کو مؤثر، قابلِ اعتماد اور شرعی و قانونی تقاضوں سے ہم آہنگ بنانے میں معاون ثابت ہو سکتا ہے۔