ISSN 1991-8976

RAJSHAHI UNIVERSITY LAW JOURNAL

FACULTY OF LAW
RAJSHAHI UNIVERSITY
2006

ARTICLES

Dower in history and it's significance in Islamic law

The Emergence of Plantation Labour in Bengal: A historical and legal study

The Convention on the Rights of the Child, 1989: Its Success or Failure after 17 years

The concept of Islamic Law and its application in Bangladesh

Hiring and Firing of Securities Regulators in Bangladesh and Australia: A Comparative Review

Rights and Care for Elderly People : Bangladesh Perspective

The Law of Maintenance and its Implementation in Bangladesh: A Comparative Study

The Nexus between Electronic and Paper Evidence under the Evidence Act, 1872

Inheritance of Orphan Grandchildren under Islamic law of Succession: A study of the impact of section 4 of the Muslim Family Laws Ordinance, 1961

পঞ্চম জাতীয় সংসদে গঠিত কতিপয় গুরত্বপূর্ণ কমিটি: একটি পর্যালোচনা

বাংলাদেশের শিকস্তি ও পয়স্তি আইন : একটি পর্যালোচনা

ইসলামে মোহরানার অধিকার ও বাংলাদেশের আর্থসামাজিক প্রেক্ষাপট ঃ একটি পর্যালোচনা

সাইবার ক্রাইম : আইন প্রয়োগ, সমস্যা ও উত্তরণের উপায় অনুসন্ধান

শিশু নির্যাতন এবং শিশু অধিকার ঃ প্রেক্ষিত বাংলাদেশ

বাংলাদেশে টিপাইমুখ বাঁধ এর প্রভাব ঃ একটি আইনী পর্যালোচনা

Abstract on the Project Legal Rights of the Child: Policy and Enforcement in Bangladesh, 1995

Scanned with CamScanner

ISSN 1991-8976

Rajshahi University Law Journal

Volume 03 2006

Published by:
Dean
Faculty of Law
Rajshahi University
Rajshahi- 6205
Bangladesh

FACULTY OF LAW
UNIVERSITY OF RAJSHAHI

Scanned with CamScanner

Rajshahi University Law Journal 2006

Editorial Board

Editor	**Professor Dr. Begum Asma Siddiqua** Dean, Faculty of Law, RU
Member	**Professor Dr. A B Siddique** Department of Law & Justice, RU
	Professor A F M Mohsin Department of Law & Justice, RU
	Dr. Mohammad Abdul Hannan Department of Law & Justice, RU
	Sayeeda Anju Department of Law & Justice, RU

Scanned with CamScanner

Rajshahi University Law Journal

FACULTY OF LAW

UNIVERSITY OF RAJSHAHI

Volume 03 2006

Published by
Dean
Faculty of Law
Rajshahi University
Rajshahi- 6205
Bangladesh

© Reserved by the Publisher

Cover Design & Printed by
B T S Commercial Institute
Benodpur Bazar, Rajshahi

Printed at:
Barendra Printing Press & Packaging
Sapora, Rajshahi

Subscription Rates
For Individuals: **Tk. 100.00 US$ 20** (without postage)
For Organisation: **Tk. 150.00 US$ 30** (without postage)

[Published in December 2006]

Scanned with CamScanner

Rajshahi University Law Journal 2006

Authors' Name	Article	Page
Dr. Begum Asma Siddiqua	Dower in history and it's significance in Islamic law	1-10
Dr. Md. Gholam Kibria	The Emergence of Plantation Labour in Bengal: A historical and legal study	11-22
Dr. Mohammad Abdul Hannan M. Ahsan Habib	The Convention on the Rights of the Child, 1989: Its Success or Failure after 17 years	23-36
Dr. Muhammad Faiz-ud-Din	The concept of Islamic Law and its application in Bangladesh	37-46
Dr. S M Solaiman	Hiring and Firing of Securities Regulators in Bangladesh and Australia: A Comparative Review	47-70
Md. Ahsan Kabir	Rights and Care for Elderly People : Bangladesh Perspective	71-84
Md. Delower Hossain	The Law of Maintenance and its Implementation in Bangladesh: A Comparative Study	85-96
Zulfiquar Ahmed	The Nexus between Electronic and Paper Evidence under the Evidence Act, 1872	97-112
Muhammad Ekramul Haque	Inheritance of Orphan Grandchildren under Islamic law of Succession: A study of the impact of section 4 of the Muslim Family Laws Ordinance, 1961	113-124
ড. রাকিবা ইয়াসমিন	পঞ্চম জাতীয় সংসদে গঠিত কতিপয় গুরুত্বপূর্ণ কমিটি: একটি পর্যালোচনা	125-144
মো. আব্দুল আলীম	বাংলাদেশের শিকস্তি ও পয়স্তি আইন : একটি পর্যালোচনা	145-156
মো. আব্দুর রহিম মিয়া	ইসলামে মোহরানার অধিকার ও বাংলাদেশের আর্থসামাজিক প্রেক্ষাপট ঃ একটি পর্যালোচনা	157-178
মুসতাক আহমেদ মো. সাহাল উদ্দীন	সাইবার ক্রাইম : আইন প্রয়োগ, সমস্যা ও উত্তরণের উপায় অনুসন্ধান	179-200
সালমা আখতার খানম	শিশু নির্যাতন এবং শিশু অধিকার ঃ প্রেক্ষিত বাংলাদেশ	201-222
মোসা. সাঈদা আঞ্জু সারাওয়াত রশীদ	বাংলাদেশে টিপাইমুখ বাঁধ এর প্রভাব ঃ একটি আইনী পর্যালোচনা	223-238
A F M Mohsin	Abstract on the Project Legal Rights of the Child: Policy and Enforcement in Bangladesh, 1995	239

Scanned with CamScanner

Rajshahi University Law Journal, 2006: **179-200**

সাইবার ক্রাইম: আইন প্রয়োগ, সমস্যা ও উত্তরণের উপায় অনুসন্ধান

মুসতাক আহমেদ*

মো: সাহাল উদ্দীন**

Abstract:

The conception of cyber crime is relating to the age of information super highway of the contemporary world. Now -a- days crimes are spreading at an alarming rate in the field of online communication system by the intellectual criminals. Through the development of technology crimes have been developing in different ways and means. So laws should be developed in such a way that crimes in the field of technological arena can be controlled in an iron hand. But no such effective legal provisions exist at home and abroad. Though there are some laws and conventions, they cannot be implemented due to some technical difficulties like procedural complexities and lack of proper execution system. Taking these advantages, the criminals are occurring heinous crimes like Hacking, Sending malicious mails, Spreading vulgar pictures, Cyber terrorism & Illegal using of intellectual properties. It causes harms to the privacy of individuals as well as creates threat to the international peace and solidarity. Now it is the demand of time to prevent such type of crimes for keeping individual's privacy as well as international peace and security. Every country of the world can enact effective legal provisions within the purview of their national boundary to protect cyber crimes. United Nations can also take necessary steps to prevent cyber crimes from the cyber space. In this Article it has tried to define cyber crime and to find out the causes of cyber crime. Nature, types & the legal provisions relating to cyber crimes are also stated in the said Article.

ভূমিকা:

"*Instantaneous global communications have given us a window on the world through which can be seen both the wonder of it all and the things that make us wonder about it all*" John Naisbitt (Global Paradox: 1994)

সাইবার অপরাধ বিশ্ব-সম্প্রদায়ের কাছে একটি প্রধান উদ্বেগের বিষয়ে পরিণত হয়েছে।[১] তথ্য-প্রযুক্তির বিস্ময়কর আবিষ্কারের কল্যাণে পৃথিবী আজ মানুষের হাতের মুঠোয়। কয়েক সেকেণ্ডের ব্যবধানে মানুষ পৃথিবীর একপ্রান্ত থেকে অপর প্রান্তে বিচরণ করছে অনায়াসেই। অসাধ্যকে করছে সাধন। এই তথ্য-প্রযুক্তির মাধ্যমে যে শুধু কল্যাণকর কাজ

---

* *সহকারী অধ্যাপক, গণযোগাযোগ-বিভাগ, রাজশাহী বিশ্ববিদ্যালয়, রাজশাহী-৬২০৫।*

** *প্রভাষক, আইন ও বিচার বিভাগ, রাজশাহী বিশ্ববিদ্যালয়, রাজশাহী-৬২০৫।*

১ This concern is shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe.

হচ্ছে এমনটি বলা যাবে না। নতুন নতুন সমস্যা ও উদ্বেগের জন্ম দিয়েছে তথ্য-প্রযুক্তি। তার মধ্যে অন্যতম এবং আলোচিত হলো সাইবার স্পেসে অপরাধ।[২]

১. সাইবার স্পেসের বিকাশ

বর্তমানে 'সাইবার স্পেস ধারণাটি সর্বাধিক আলোচিত বিষয়। এ সম্পর্কে সর্বপ্রথম ধারণা দেন উইলিয়াম গিবসন নামে একজন কল্পকাহিনী লেখক। তার *'নিউ রোম্যান্সার'* উপন্যাসে তিনি বলেন 'সাইবার স্পেস ...প্রত্যেক জাতির বিলিয়ন বিলিয়ন উত্তরাধিকার এবং তাদের প্রাপ্ত ব্যবহারকারীর প্রাত্যহিক অভিজ্ঞতা এক ঐক্যবদ্ধ মায়া (হ্যালুসিনেশন)। শিশুরা শিখে চলেছে গণিত ... মানবীয় সিস্টেমের প্রত্যেক কম্পিউটার ব্যাংক থেকে আহরিত তথ্যের গ্রাফিক্স পরিবেশনা। অচিন্তনীয় জটিলতা। মানব মনের কাল্পনিক এলাকা। সংগঠিত তথ্য মহা সমুদ্র থেকে বিচ্ছুরিত আলোকরশ্মি ...শহরে আলোর বন্যার মতো ...'।[৩] উইলিয়ম গিবসনের উপন্যাসের সাথে বর্তমানের বাস্তবতার এক দারুন মিল লক্ষ করা যায়। কেননা আজকে একটি শিশু কেবল তিন মাইল দুরের একটি স্কুলেই যাচ্ছে না, ঘরে বসেই তিন হাজার মাইল দুরের কোন এক স্কুলের পাঠ সে গ্রহন করছে। একজন ব্যবসায়ী আজ তার পণ্যের পসার নিয়ে নির্দিষ্ট কোন বাজারে বসছে না, সে ব্যবসা করছে বিশ্বময়। একজন চোর আজ সিঁধ কেটে চুরি করছে না, ঘরে বসেই বিশ্বের যে কোন প্রান্তের কোটি টাকার সম্পদ সে নিজের আয়ত্তে আনছে। একজন সন্ত্রাসী শুধু নিজ এলাকাতেই ত্রাস সৃষ্টি করছে না, খুব সহজেই সারা বিশ্বে সে ত্রাসের কারণ হয়ে দাঁড়াচ্ছে। আর এ সবই সম্ভব হচ্ছে সাইবার স্পেস নামক খোলা আকাশে।

জনৈক লেখক[৪] সাইবার স্পেস বলতে মনে করেন 'For jurisdictional analysis, cyber space should be treated as a fourth international space.' তিনি আরও বলেন, Cyber space is a virtual place beyond the boundaries that can easily be considered as an international territory.' কিন্তু প্রশ্ন হলো, সে সাইবার স্পেসটা কোথায়? এর উত্তরে বলা যায় – এটা একটা অধিসত্ত্বা; যা সর্বময় বিরাজমান অথবা এর অস্তিত্ব কোথাও নেই। যদি তাই হয় তবে সাইবার স্পেস জিনিসটাই বা কী? এর উত্তরে বলা যায়, এর কাজের ধরনটাই শুধু ব্যাখ্যা করা সম্ভব। কার্যত: সাইবার স্পেস এমন একটা স্থান যার মাধ্যমে বার্তা এবং ওয়েব পেজ পৃথিবীর যে কোন জায়গায় পাঠানো

২ D. Parker, *Fighting Computer Crime: For Protecting Information*, U.S.A, John Wiley, 1998, p. 10.

৩ Gibson W. *Neuromancer*, Newyork, Grafton, 2001 p.1.

৪ D. Johnson and D. Post, *Law and Borders: The Rise of Law in Cyberspace* (Stamford, Stamford Law Review), [1996], p. 1378.

Scanned with CamScanner

সম্ভব। আবার মার্কিন যুক্তরাষ্ট্রের সুপ্রিম কোর্টের মতে – Cyber space is a place outside national boundaries."[৫]

আক্ষরিক অর্থে সাইবার বলতে 'Cybernetics' বিজ্ঞানকে বুঝায়। গ্রীক শব্দ 'Kubernao' থেকে 'Cybernetics' শব্দটি এসেছে যার অর্থ–হাল ধরা বা শাসন করা। বর্তমানে যেটা পরিচালনা করা অর্থে ব্যবহৃত হয়।[৬] আসলেই তাই। সাইবার স্পেসের মাধ্যমেই আজ আমাদের সব কিছু নিয়ন্ত্রিত হচ্ছে। সর্বোপরি, 'আমরা যা দেখি বা পর্যবেক্ষণ করি, ঐ বিষয় নিয়ে তার চেয়েও বেশি চিন্তা করি তা-ই সাইবার স্পেসের মূল কথা।[৭]

২. সাইবার ক্রাইম

'সাইবার স্পেস' মানব সভ্যতা উন্নয়নের এক উন্মুক্ত পথ হলেও আজ তা অপরাধ কর্মকাণ্ডের আখড়া হিসেবে চিহ্নিত হচ্ছে। এখন প্রশ্ন হলো – অপরাধ কী? কিংবা সাইবার অপরাধ-ই বা কী? এসব অপরাধগুলো কার বিরুদ্ধে এবং কেনই বা সংগঠিত হচ্ছে। সাধারণ ভাষায় বলতে গেলে, আইন বিরুদ্ধ, নীতি বিবর্জিত, সামাজিক মূল্যবোধকে আঘাত করে সে ধরনের কর্মকাণ্ড যার জন্য শাস্তি পেতে হয় তা-ই অপরাধ। সাইবার ক্রাইম হচ্ছে এমন এক ধরনের অপরাধ যা সমগ্র বিশ্বকে স্পর্শ করে। ইউরোপীয়ান রিপোর্টে ব্যাপারটাকে ব্যাখ্যা করা হয় এভাবে – 'Computer related crimes are committed across cyber space and don't stop at the conventional state- borders. They can be perpetrated from any where and against any computer user in the world.'[৮]

৩. সাইবার ক্রাইমের ধরন

সাইবার ক্রাইম ধারণাটি বেশ জটিল। অনেক ক্ষেত্রে বিভ্রান্তিমূলকও বটে। একে সার্বজনীন কোন কাঠামোতে ব্যাখ্যা করা যায় না। তারপরও নিম্নলিখিত অপরাধের ধরনগুলো সাইবার ক্রাইমকে তুলে ধরতে সহায়তা করে।

ক.হ্যাকিং এবং এর সাথে সংশ্লিষ্ট কর্মকাণ্ড।

খ. ভাইরাস এবং বিদ্বেষমূলক বার্তা ছড়ানো।

গ. অনলাইন প্রতারণা:

---

৫ Ibid.

৬ রহমান, মোহাম্মদ মাহাবুবুর, সাইবার স্পেসঃ ক্লেইমিং চেঞ্জ ইন ট্রেডিশনাল কনসেপ্টস অব জুরিসপ্রুডেন্স, ঢাকা, ২০০৫, পৃঃ ৩৭।

৭ *কম্পিউটার টুমরো*, বর্ষ:৪, সংখ্যা ৩, জানুয়ারী ২০০৩, পৃ. ৮।

৮ Chawki Mohamed, A Critical Look at the Regulation of Cybercrime. 2005 www.crime-research.org/articles/Critical/

১. কম্পিউটার ব্যবহারে প্রতারণা;
২. কম্পিউটার ব্যবহারে জালিয়াতি;
৩. বিভিন্ন ডাটা ও প্রোগ্রামের পরিবর্তন সাধন;
৪. ই-মেইলের মাধ্যমে জালিয়াতি।

ঘ. অশ্লীল বার্তা পাঠিয়ে হয়রানি।
ঙ. সাইবার টেরোরিজম।
চ. হ্যাক্টিভিজম।
ছ. পর্ণোগ্রাফির প্রসার।
জ. বুদ্ধিবৃত্তিক সম্পদের অবৈধ ব্যবহার।

ক. হ্যাকিং এবং এর সাথে সংশ্লিষ্ট কর্মকাণ্ড

'হ্যাকিং' বলতে সাধারণত 'ইন্টেলিজেন্ট ক্রিমিনাল'দের কৃতকর্মকেই বুঝায়। আর এই ইন্টেলিজেন্ট ক্রিমিনালদের কাজই হলো কমপিউটার সিস্টেমে প্রবেশ করে বিভিন্ন ডাটা, প্রোগ্রামের কার্যকারিতা নষ্ট করে দেওয়া এবং ক্ষতিকর ভাইরাস সৃষ্টি করা।

OXFORD Advanced Learner's DICTIONARY (1998) তে হ্যাকারের সংজ্ঞায় বলা হয়েছে–
'A person who spends a lot of time using Computers for a hobby, especially to look at data without permission.'

The New Hackers Dictionary[৯] তে হ্যাকিং এবং হ্যাকারের সংজ্ঞায় বলা হয়েছে–

১. 'হ্যাকার' হলো তারাই যারা প্রোগামোপযোগী পদ্ধতির বিস্তার খুঁজতে পছন্দ করে এবং ব্যবহারকারীদের সমস্যা সৃষ্টি করে। তারা এর গুরুত্ব বোঝে না।
২. ঐ ব্যক্তি যিনি বুদ্ধিবৃত্তিক প্রতিযোগিতা পছন্দ করে এবং কৌশলের মাধ্যমে অন্যকে ফাঁদে ফেলে।
৩. হ্যাকার' হচ্ছে একজন দক্ষ প্রোগ্রামার।
৪. নির্দিষ্ট ভাষায় কুশলী।
৫. একজন অনধিকারচর্চাকারী হিংসুটে যে সংবেদনশীল তথ্যসমূহ খুঁজে বের করতে চেষ্টা করে।
৬. প্রোগ্রামিংয়ে কৌতুহলী।

---

৯ E. Raymond, *The New Hackers Dictionary* (U.S.A, MIT Press), 2003, p. 19

তাই বলা যায়, 'হ্যাকার হলো তারাই যারা বিভিন্ন কমপিউটার সিস্টেমে অনুপ্রবেশ করে এবং তাদের একমাত্র উদ্দেশ্য হচ্ছে জ্ঞান বৃদ্ধি ও তথ্যের তৃষ্ণা মেটানো।'[১০]

হ্যাকার: ক্ষতিসাধনকারীর অপর নাম

স্পাইওয়্যার নামে এমন একটি প্রোগ্রাম রয়েছে যা নজরদারি করে ইন্টারনেটসহ কমপিউটারের যাবতীয় কার্যক্রম। এই প্রোগ্রামটি ইন্টারনেট ব্যবহারের সময় অবিরাম বর্ষণ করবে বিজ্ঞাপন; কমপিউটারকে পরিণত করবে ভাইরাসের শিকারে। কমপিউটারের গতি অনেক কমিয়ে ফেলে। স্পাইওয়্যার এমনিতেই কমপিউটারে ইনস্টল হয়ে যায় এবং নেপথ্যে থেকে কাজ করতে থাকে। প্রোগ্রামটির মূখ্য উদ্দেশ্য হলো ইন্টারনেটে ব্যাক্তিগত তথ্য যেমন: কোন্ সাইট খোলা হয়েছে, ক্রেডিট কার্ড নম্বর, ই-মেইল পাসওয়ার্ড এমন কি যে কি-বোর্ডে টাইপ করা হচ্ছে তার সবকিছু সংগ্রহ করা। স্পাইওয়্যারের ফলাফল আরও খারাপ হয় যখন ব্যাক্তিগত তথ্যগুলো ইন্টারনেট সংযোগের মাধ্যমে চুপিচুপি চলে যায় কমপিউটার হ্যাকারদের কাছে। এর ফলে স্পাইওয়্যার ব্যবহারকারীরা কমপিউটার ব্যবহারকারীর পরিচয়ের আড়ালে যে কোন অপকর্ম করতে পারে। যেমন: আপনার ই-মেইল বা মেসেঞ্জার অ্যাকাউন্ট ব্যবহার করে অন্যদের কাছে ই-মেইল বা তাৎক্ষনিক বার্তা পাঠাতে পারা যায় অথবা ক্রেডিট কার্ড, ব্যাংকের হিসাববিষয়ক তথ্য ব্যবহার করে আপনার অর্থ আত্মসাৎ করতে পারবে। এছাড়াও এসব ইন্টারনেট ব্যবহারের প্রোগ্রাম থাকা 'হোম সাইট' এর ঠিকানাও বদলে দিতে পারে। গত আগস্টে মার্কিন কেন্দ্রীয় বাণিজ্য কমিশন বিষয়ক একটি কর্মশালায় মাইক্রোসফট জানিয়েছে, যতগুলো উইন্ডোজ অপারেটিং সিস্টেম নষ্ট হয়ে যায় (ক্র্যাশ) তার অর্ধেকের কারণ স্পাইওয়্যার। কিন্তু ব্যবহারকারীরা বেশিরভাগ ক্ষেত্রেই বুঝতে পারেন না মূল কারণটি কী। যুক্তরাষ্ট্রে ওয়েবরুট সফটওয়ার আর্থলিঙ্ক সাড়ে ৬ লাখ কমপিউটারের উপর গবেষণা করে দেখেছে, এসবের মধ্যে ১৮ লাখ স্পাইওয়্যার ছিল।[১১] ২০০৫ সালের ১ মার্চ থেকে ৩০ এপ্রিলের মধ্যে তারা এই গবেষণাটি চালিয়েছিল। এরপর জুন মাসে আর্থলিঙ্ক তাদের নেটওয়ার্কে থাকা কয়েক হাজার কমপিউটারের উপর এ গবেষণা চালিয়ে দেখতে পেয়েছে যে, গড়ে প্রতিটি কমপিউটারে ২৮ টি করে স্পাইওয়্যার রয়েছে।[১২]

---

১০ *কম্পিউটার টুমরো*, বর্ষ: ৪, সংখ্যা ৫, মার্চ ২০০৪, ঢাকা, পৃ: ৭।

১১ A. Nagpal, *Cyberterrorism in the Context of Globalisation* (India, UGC sponsored National Seminar held in New Delhi on Globalization and Human Rights), [September 2001].

১২ রহমান, মোহাম্মদ মাহাবুবুর, প্রাগুক্ত, পৃ: ৩৯।

Scanned with CamScanner

একই ধরনের আরেকটি প্রোগ্রাম হলো অ্যাডওয়্যার। এটি কমপিউটার ব্যবহারকারীর ব্যক্তিগত পছন্দ-অপছন্দ বিষয়গুলো জানিয়ে দেয় বিভিন্ন বিজ্ঞাপনী সংস্থাকে। সংস্থাগুলো সেসব তথ্যকে ভিত্তি করে বেছে বেছে বিজ্ঞাপনের বোমা বর্ষণ করে। যেমন: কেউ যদি নিয়মিত গাড়ি বিক্রেতাদের ওয়েবসাইট দেখেন তবে অ্যাডওয়্যারটি কমপিউটারে অন্যান্য গাড়ি বিক্রেতাদের বিজ্ঞাপন দেখাবে।[১৩]

হ্যাকার : ক্ষতির আলোকে কিছু পরিসংখ্যান

কমপিউটার ইমারজেন্সি রেসপন্স টিমের রিপোর্ট অনুযায়ী, ১৯৯৯ সালে আমেরিকাতে হ্যাকারদের সংঘবদ্ধ আক্রমণের প্রায় পাঁচ হাজারটি ঘটনা ঘটেছে। আর ২০০০ সালে এ ধরণের অপরাধের পরিমাণ বেড়ে গিয়ে দাঁড়িয়েছিল প্রায় সতেরো হাজারে। ২০০১ সালে তো সাইবার ক্রাইম বেড়ে গিয়ে আমেরিকাতেই পঞ্চাশ হাজারকে পার করেছিল। এফবিআইয়ের হিসাব আনুযায়ী, অভ্যন্তরীণ ও বহিরাগত নিরাপত্তা ভঙ্গ সংক্রান্ত কারণে ২০০৪ সালে ক্ষতির পরিমাণ বিলিয়ন বিলিয়ন ডলারকে ছাড়িয়েছে।

বাংলাদেশেও এখন হ্যাকিংয়ের মতো ঘটনা ঘটে চলেছে। বছর পাঁচেক আগে ব্রাক ব্যাংকের হ্যাকিংটি সারা বিশ্বে আলোচিত হয়েছিল। এমনিভাবে ঢাকা স্টক এক্সচেঞ্জ এ ট্রানজেকশন রিপোর্ট চুরি করার জন্য তাদের কমপিউটার হ্যাক করা হয়েছিল। আবার একদল হ্যাকার বাংলাদেশের জাতীয় সংসদের ওয়েবসাইটটি হ্যাক করে সেখানে নীল ছবিতে ভরপুর করে তুলেছিল। ২০০৪ সালে দেশীয় ওয়েবসাইট আওতায় বায়লা ডট কমও হ্যাকিংয়ের শিকার হয়েছিল।[১৪]

গ. ভাইরাস এবং বিদ্বেষমূলক বার্তা ছড়ানো

ভাইরাস (VIRUS)-এর অভিধানিক অর্থ হলো 'সংক্রামক'। রোগ সংক্রান্ত বিষয়ে যখন ভাইরাস কথাটি ব্যবহার করা হয় তখন এর দ্বারা সহজেই জীববিজ্ঞানিক ভাইরাসকে অনুমান করা হয়। ধুলাবালি নিশ্বাস-প্রশ্বাসের সাথে যে জীবাণু সংক্রামিত হয়ে থাকে তা জীববিজ্ঞানিক ভাইরাস। তবে কমপিউটার ভাইরাস জীববিজ্ঞানিক ভাইরাস নয়। এটি ছোট একটি প্রোগ্রাম বা সফটওয়্যার। এ ভাইরাস প্রোগ্রামটি এক কমপিউটার থেকে অন্য কমপিউটারে যে কোন প্রোগ্রাম স্থানান্তর, ই-মেইল ইন্টারনেট থেকে প্রোগ্রাম ডাউন লোড, ফ্লপি ডিস্ক, কমপ্যাক্ট ডিস্ক ইত্যাদি ব্যবহারের সময় স্থানান্তরিত হয়। কমপিউটার উদ্ভাবনের পর থেকে মানুষ কমপিউটারকে মানুষের সাথে তুলনা করে আসছে।

---

১৩ *দৈনিক প্রথম আলো*, ২৯ অক্টোবর ২০০৪, পৃ: ৭।

১৪ কে. এম. শামীম হায়দার, সাইবার অপরাধ সতর্ক হওয়ার এখনই সময়, *দৈনিক ভোরের কাগজ*, ১০ জানুয়ারী ২০০৫, পৃ: ১১।

কমপিউটারের অনেক যন্ত্রপাতির পরিভাষায় মানুষের দৈহিক পরিচয়ের সঙ্গে মিল রেখে নাম রেখেছে। তার মধ্যে ভাইরাস একটি নাম। কমপিউটার প্রোগ্রামাররা এ সমস্ত ভাইরাস প্রোগ্রামগুলো তৈরি করেন।

ঘ. ভাইরাস : সংজ্ঞা ও ধারনা ব্যাপক

১৯৮৪ সালে ফেড কোপেন ভাইরাসের প্রথম সংজ্ঞা প্রদান করেন। তিনি বলেন, 'ভাইরাস হচ্ছে এমন একটি প্রোগ্রাম যা অন্য কোন প্রোগ্রামের সাথে যুক্ত হয়ে কমপিউটারের ক্ষতি সাধন করে।'[১৫]

সাইম্যানটেক কোম্পানিও ভাইরাসের একটি সংজ্ঞা দেয় যেখানে বলা আছে– 'ভাইরাস হচ্ছে এমন এক প্রোগ্রাম যা নিজেই নিজের প্রতিরূপ তৈরি করে বিভিন্ন ফাইল, বুট সেক্টর বা র‍্যামে সংযুক্ত থাকে। এটি ব্যবহারকারীর অগোচরে কমপিউটারে প্রবেশ করে এবং দ্রুত বিস্তার লাভ করতে থাকে।'[১৬]

OXFORD Advanced Learner's DICTIONARY (1998) তে ভাইরাসের সংজ্ঞায় বলা হয়েছে– '. . . instructions that are hidden within a Computer Program & are designed to cause faults or destroy data.'

অতএব বলা যায় যে, ভাইরাস একটি ছোট প্রোগ্রাম যা অন্য প্রোগ্রামের সাথে কমপিউটারে প্রবেশ করে। প্রোগ্রামটি যদি বুট সেক্টরের জন্য তৈরি করা হয় তাহলে বুট সেক্টরে কাজ করবে। প্রোগ্রাম বা হার্ডওয়্যারের অংশের জন্য তৈরি করা হলে কমপিউটারে সে অংশে স্থাপিত হয়ে যাবে। তারপর ভাইরাস প্রোগ্রামের নির্দেশ অনুযায়ী কার্যক্রম শুরু করবে। অনেক সময় বলা হয়, হার্ডডিস্কে ভাইরাস আক্রমন করেছে। আসলে হার্ডডিস্কের মধ্যেই সকল সফটওয়্যার থাকে বিধায় হার্ডডিস্কের কথা বলা হয়।

উপরের সংজ্ঞাগুলোর আলোকে ভাইরাসের কয়েকটি উল্লেখযোগ্য বৈশিষ্ট্য সম্পর্কে নীচে আলোচনা করা হলো:

ক) কমপিউটার ভাইরাস নিজেই নিজের প্রতিরূপ তৈরি করতে সক্ষম।

খ) এটি সর্বদা অন্য কোন ফাইল বা প্রোগ্রামের সাথে চলাফেরা করে।

গ) সকলের অগোচরে এটি অন্য কোন ফাইল বা প্রোগ্রাম বা সিস্টেমে বিস্তার লাভ করতে পারে।

ঘ) বেশ কিছু ভাইরাস আছে যেগুলো খুব দ্রুত বিস্তার লাভ করতে পারে। এইসকল ভাইরাসকে খুব সহজেই চিহ্নিত করা যায়। যেমন: 'লাভ বাগ'।

---

১৫ শোয়েব হাসান খান,'ভাইরাস: প্রতিকার ও প্রতিরোধের সহজ', *মাসিক কম্পিউটার জগৎ*, বর্ষ: ১০ সংখ্যা-২ জুন ২০০০, পৃ. ৩৫।

১৬ প্রাগুক্ত শোয়েব হাসান খান, পৃ. ৩৫।

Scanned with CamScanner

ঙ) আবার অনেক ভাইরাস আছে যেগুলো নিজেকে লুকিয়ে রাখে। ফলে এন্টি-ভাইরাস সফটওয়্যারগুলো সহজে এদের চিহ্নিত করতে পারে না। যেমন: ১৯৮৬ সালের 'ব্রেইন'।

অ. ভাইরাস: শুরুটা কীভাবে?

১৯৪০ সালের দিকে গণিতবিদ জন ভন নিউম্যান সর্বপ্রথম সেলফ-রেপলিকেটিং (নিজে নিজে বংশবৃদ্ধি করতে পারে এমন) গাণিতিক মেকানিজমের উপর গবেষণা পরিচালনা করেন। তত্ত্বগতভাবে এসব রিপ্রাডিউসিং অপারেশনগুলো স্বয়ংক্রিয়ভাবে কিছু পূর্ব নির্ধারিত কার্য সম্পাদন করতে সক্ষম।

এরপর থেকে বিভিন্ন ধরনের গবেষণা কাজে নিয়ন্ত্রিতভাবে এসব সেলফ-রেপলিকেটিং প্রোগ্রাম ব্যবহার হচ্ছিল। তবে ৮০'র দশকের শুরুর দিক পর্যন্ত এগুলোর ব্যবহার কমপিউটার পেশাজীবীদের মধ্যেই সীমাবদ্ধ ছিল। এরপর পরই মূলত প্রথম কমপিউটার ভাইরাসের উদ্ভাবন হয় যার নাম 'Elk Cloner' এবং এটি তখনকার বহুল ব্যবহৃত 'Apple 2' কমপিউটারের জন্য প্রযোজ্য ছিল। এর কয়েক বছর পরেই ১৯৮৬ সালে প্রথম আইবিএম পিসি ভাইরাসের সৃষ্টি হয় যার নাম 'ব্রেইন'। আমেরিকার ন্যাশনাল ইনস্টিটিউট অব স্ট্যান্ডার্ড এন্ড টেকনোলজি বা এনআইএসটি'র মতে এই ভাইরাসটি প্রাথমিকভাবে ডেলওয়ার ইউনিভার্সিটিতে ডিস্কেটের মাধ্যমে বিস্তার লাভ করে। এরপরের বছরই বাজারে এন্টি-ভাইরাস সফটওয়্যার বের হয়।

আ. ভাইরাস : বিভিন্ন ধরন-কার্যক্ষমতা

বিশ্বজুড়ে হাজার হাজার কমপিউটার ভাইরাস প্রোগ্রাম ছড়ানো হয়েছে। এক একটি কমপিউটার ভাইরাস প্রোগ্রামের কার্যক্রম এক এক রকম। এ ধরনের কয়েকটি উল্লেখযোগ্য ভাইরাস হলো: 'মিলেনিয়াম বাগ', 'Y2K','চেরনোবিল', 'মায়া', 'লাভ বাগ', 'মেলিসা', 'জেডিবিজিএমজিআর ডট ইএক্সই', 'লিরভা', 'w 32/Amus-A' ইত্যাদি।

মিলেনিয়াম বাগের ছোট্ট একটা ধাক্কাতেই বিশৃঙ্খলা দেখা দেয় বিশ্বের ৮৬,০০০ বাণিজ্যিক জাহাজে।[১৭] ঠিক কোর্স ধরে ভেসে যাওয়া, অন্য জাহাজ বা বন্দরের সাথে যোগাযোগ রক্ষা করা বা সময়মতো স্পীড বাড়ানো-কমানোর ক্ষেত্রে সমস্যা হয়ে থাকে। ফলে কোটি কোটি টাকার শিল্পপণ্য, খাদ্য, জ্বালানির পরিবহন পুরোপুরি বিঘ্নিতও হতে পারে। মুখোমুখি সংঘর্ষে প্রাণহানির আশংকা তো রয়েছেই।

'টাস্কফোর্স ২০০০' নামের যুক্তরাজ্যভিত্তিক একটি সংস্থা- জার্মানি, স্পেন, ইটালি, পর্তুগাল, ফিনল্যান্ড, সুইজারল্যান্ড, চেক প্রজাতন্ত্র, হাঙ্গেরি, পোলান্ড এবং রাশিয়াকে 'রেড

---

১৭ শামীম আখতার তুষার, 'প্রযুক্তির ভয়াবহতম বিপর্যয় Y2K কি অঘটন ঘটবে' *মাসিক কমপিউটার জগৎ*, বর্ষ: ০৯, সংখ্যা ০৮, ডিসেম্বর ১৯৯৯, পৃ: ৯।

লাইট জোন' হিসেবে অভিহিত করেছে। কারণ এ সমস্ত দেশের বিমান সংস্থা থেকে Y2K সমস্যামুক্তি সম্পর্কে যে খবর পাওয়া গেছে, তা মোটেই যথেষ্ট ও সন্তোষজনক নয়। এই ১০টি দেশে বিমান ভ্রমণের সময় যে কোন মুহূর্তে প্লেন ক্র্যাশের সম্ভাবনা রয়েছে। এছাড়াও এই সংস্থাটি এম্বার (হলুদাভ) এবং গ্রীণ জোন নামে আরও দু'টো বিমান ভ্রমণ অঞ্চলের রেটিং প্রকাশ করেছে। এম্বার এলাকার দেশগুলোর মধ্যে অস্ট্রেলিয়া, অস্ট্রিয়া, বেলজিয়াম, কানাডা, ফ্রান্স, গ্রীস, আইসল্যান্ড, ভারত, আয়ারল্যান্ড, জাপান, নেদারল্যান্ড, নিউজিল্যান্ড, দক্ষিণ আফ্রিকা আর তুরস্ক অন্তর্ভুক্ত। এ সমস্ত দেশে প্লেন ক্র্যাশের সম্ভাবনা না থাকলেও অন্তত দীর্ঘ সময়ের জন্য অনির্ধারিত যাত্রাবিরতি বা বিমান বন্দরে আটকে পড়ার যথেষ্ট সম্ভাবনা রয়েছে। চীন, ডেনমার্ক, মিশর, হংকং, ইসরায়েল, সুইডেন এবং যুক্তরাজ্য গ্রীণ জোন হিসাবে পরিচিত।

যুক্তরাষ্ট্র সম্পর্কে যুক্তরাজ্যের এই সংস্থার বিশ্লেষণ না পাওয়া গেলেও আরও অনেক সংস্থা থেকে জানা গেছে Y2K নিয়ে গোটা যুক্তরাষ্ট্রে বিরাজমান দুশ্চিন্তা, উদ্বেগ আর সাবধানতার কথা। কমপিউটারের ভুলের কারণে যুক্তরাষ্ট্র থেকে মেক্সিকোতে প্রায় ২ লক্ষ ৪০ হাজার জুতা ডান আর বাম পায়ের পাটি উল্টা-পাল্টা করে সরবরাহ করা হয়। যুক্তরাষ্ট্রের ভিতরে ও বাহিরে প্রায় ১ লক্ষ ২০ হাজার কপি বই ছাপিয়ে বাজারে দেওয়া হয় যার প্রতিটির প্রচ্ছদ ভুল। সম্প্রতি কংগ্রেসের কাছে প্রদত্ত রিপোর্টে উল্লেখ করা হয়েছে, Y2K সমস্যার কারণে সে দেশের বিভিন্ন হাসপাতালে হাজার হাজার বায়োমেডিক্যাল ডিভাইস নষ্ট হয়ে গেছে। এছাড়াও কয়েক হাজার বায়োমেডিক্যাল প্রোডাক্টও Y2K সমস্যামুক্ত নয় বলে ধরা পড়েছে। এর ফলে হাজার হাজার হৃদরোগী আর সদ্যজাত শিশু মৃত্যুর কোলে ঢলে পড়েছে। শুধু এতটুকুই নয়, এখানে প্রায় ৬০ হাজার ক্রেডিটকার্ড ভুল তথ্য দিয়েছে। যুক্তরাষ্ট্রে এখনো Y2K সংক্রান্ত প্রায় ৭০টি মামলা বিচারাধীন রয়েছে। যত দিন যাবে এ নিয়ে মামলার সংখ্যা ততই বাড়বে এবং বিশেষজ্ঞদের ধারণা এ সংক্রান্ত মামলার পেছনে প্রায় ১ ট্রিলিয়ন ডলার খরচ হবে যুক্তরাষ্ট্র সরকারের। এটা অবশ্যই তাদের অর্থনীতির উপর বিরাট প্রভাব ফেলবে।[১৮]

---

১৮ প্রাগুক্ত শোয়েব হাসান খান, পৃ. ৩৫

অধিকাংশ কমপিউটার নিরাপত্তা বিশেষজ্ঞদের মতে, ক্ষতি এবং বিস্তারের দিক দিয়ে 'লাভ বাগ' বিশ্বের এক নম্বর ভাইরাস। ফিলিপাইনের কিউজোন শহরের একটি আইএসপি'র সার্ভারে সর্বপ্রথম এটি আত্মপ্রকাশ করে এবং কয়েক ঘন্টার মধ্যে এশিয়া, ইউরোপ ও আমেরিকায় ছড়িয়ে পড়ে।[১৯]

লাভ বাগ ভাইরাসের পরে সবচেয়ে দ্রুত বিস্তার করা ভাইরাসটি হলো 'মেলিসা ম্যাক্রো ভাইরাস'। এটি ডিস্কেট বা ফাইল ডাউনলোড বা ই-মেইল এটাচমেন্টের মাধ্যমে ছড়িয়ে পড়ে। এ ভাইরাসের মাধ্যমে ম্যাক্রো ফাংশন সাপোর্ট করে এ ধরনের ডকুমেন্ট, ফাইল, স্প্রেডশিট ও ডাটাবেসগুলোই শুধু আক্রান্ত হয়।

ই-মেইলের মাধ্যমে যুক্তরাষ্ট্রে 'জেডিবিজিএমজিআর ডট ইএক্সই' এবং 'লিরভা' নামে দুটি ভাইরাস ছড়িয়ে পড়ে লাখ লাখ কমপিউটার সিস্টেম ধ্বংস করে দিয়েছে। কোস্টারিকায় বেশিরভাগ কমপিউটার আক্রান্ত হয়েছে জেডিবিজিএমজিআর ডট ইএক্সই ভাইরাসে আর লিরভা ভাইরাস ছড়িয়ে পড়েছে ল্যাটিন আমেরিকার বিভিন্ন দেশের কমপিউটারে। লিরভা ভাইরাসটি এর আগে ছড়িয়ে পড়েছিল ব্রাজিল, ইটালি, ব্রিটেন, শ্রীলঙ্কা ভারত, যুক্তরাষ্ট্র এবং স্পেনের লাখ লাখ কমপিউটারে।[২০]

'সফোস' নামক ইন্টারনেট নিরাপত্তা প্রতিষ্ঠানের বিশেষজ্ঞরা সম্প্রতি 'w 32/Amus-A' নামে এমন একটি ভাইরাস খুঁজে বের করেন যা কথা বলতে পারে। এই ওয়ার্মটিও ই-মেইলের মাধ্যমে ছড়িয়ে পড়ে। ই-মেইলটির বিষয়বস্তুতে লেখা থাকে 'শোনো আর হাসো'। উইন্ডোজ ব্যবহারকারীরা ই-মেইলটি খোলার সাথে সাথে আক্রান্ত হন এবং তার মাধ্যমে ভাইরাসটি ছড়িয়ে পড়ে।

ই. ভাইরাস : কিছু পরিসংখ্যান

- ১৯৯১ সালে মোট ভাইরাসের সংখ্যা ছিল ১,০০০। ১৯৯৭ সালে এ সংখ্যা বেড়ে ২০,০০০ ছাড়িয়ে যায়। আর বর্তমানে ৪৫,০০০-এরও বেশি ভাইরাস রয়েছে।
- এক জরিপ মতে, কোম্পানিগুলোতে প্রতি বছর গড়ে ৮১ বার ভাইরাস আক্রমণের ঘটনা ঘটে।
- সকল কমপিউটার ব্যবহারকারীরা ১২% ভাইরাস দ্বারা আক্রান্ত হয়।

---

১৯ প্রাগুক্ত শোয়েব হাসান খান, পৃ. ৩৫।

২০ মাসিক *কমপিউটার টুমরো*, বর্ষ: ০৪, সংখ্যা ০৪, ফেব্রুয়ারি ২০০৩, পৃ. ২১।

Scanned with CamScanner

□□ ১৯৯৯ সালের প্রথম ছয় মাসে বিভিন্ন ভাইরাস দ্বারা সংঘটিত ক্ষয়ক্ষতির পরিমাণ ছিল ৭৬০ কোটি।[২১]

গ. অনলাইন প্রতারণা

অপরাধ সংঘঠনের ক্ষেত্রে কম্পিউটার অপারেটিং এর সকল ক্ষেত্রেই সংবেদনশীল; যা প্রতারণার লক্ষ্য, প্রতারণার উপাদান অথবা উভয়ক্ষেত্রেই ব্যবহৃত হয়। ডাটা ইনপুট, আউটপুট, প্রক্রিয়াজাতকরণ এবং জ্ঞাপন সবকিছু অসৎ উদ্দেশ্য ব্যবহৃত হয়। কম্পিউটারের মাধ্যমে প্রতারণার সাধারণ ধরনগুলো নিচে আরোচনা করা হল–

অ. কম্পিউটার ব্যবহারে প্রতারণা

ব্যাংকে গচ্ছিত সম্পদ, কার্যকাল ইত্যাদির ভূয়া হিসাব উপস্থাপন কম্পিউটার প্রতারণার সবচেয়ে সাধারণ উদাহরণ। আরও আছে গ্রাহকদের অর্থনৈতিক ও ব্যক্তিগত তথ্যসমূহ স্থানান্তরকরণ। কম্পিউটার প্রতারণার সবচেয়ে লাভজনক খাত হিসেবে ভ্রমণ সম্পর্কিত তথ্য ও ক্রেডিট কার্ড জালিয়াতি অন্যতম। ডাটা বেইজে অত্যন্ত দক্ষতার সাথে প্রবেশ করে হ্যাকাররা প্রোগ্রামের ইনপুট আউটপুট নিয়ন্ত্রণ করে। এভাবেই যুক্তরাষ্ট্রের ফ্লোরিডায় ৫০ মিলিয়ন ডলারের একটি ভূয়া লেনদেন হয়েছিল। এছাড়াও ইউরোপের দেশগুলোতে এগুলো নিত্যনৈমত্তিক ঘটনা।[২২]

আ. কম্পিউটারে জালিয়াতি

কোন কম্পিউটার সিস্টেমে সংরক্ষিত তথ্যের বিকৃতি ঘটানোই কম্পিউটার জালিয়াতি; যেটাতে হ্যাকাররা যথেষ্ট পারদর্শী। বিশ্বের যে কোন কম্পিউটারই হ্যাকারদের জালিয়াতির শিকার হতে পারে। কম্পিউটারাইজড কালার লেজার কপির সহজলভ্যতাই কোন তথ্য-উপাত্তের প্রতিলিপি সৃষ্টির সহায়ক যা গ্রাহকদের তথ্য সংরক্ষণের ক্ষেত্রে যথেষ্ট আশঙ্কাজনক। একজন দক্ষ হ্যাকার এমন ধরনের ডকুমেন্ট তৈরি করে যার সত্যতা যাচাই করা অসম্ভব। এভাবেই তৈরি হয় জাল নোট, সনদপত্র এবং হ্যাকারদের প্রয়োজনীয় দলিলপত্র।

ঘ. অশ্লীলবার্তা পাঠিয়ে হয়রানি

সময়ের দ্রুততার সাথে প্রযুক্তির উন্নয়নও সমানতালে এগিয়ে চলেছে। সাইবার স্পেস বা ইন্টারনেট হলো তথ্য প্রযুক্তির বিস্ময়কর বিপ্লবেরই একটি অন্যতম আবিষ্কার। এ সম্পর্কে পূর্বে বিস্তারিত আলোচনা করা হয়েছে। বলা হয়েছে সাইবার ক্রাইমের বিভিন্ন ধরনও। এ ধরনগুলোর অন্যতম একটি সাইবার স্পেস ব্যবহার করে মেয়েদের হয়রানি। প্রয়োজনের

---

২১ প্রাগুক্ত, শোয়েব হাসান খান, পৃ.৩৫।

২২ J. Wells, *The Computer and Internet Fraud Manual* (Austin, Texas), [2002] p. 3.

তাগিদে যুগের চাহিদায় সাইবার স্পেসের বিশাল জগতে অংশ গ্রহণ বৃদ্ধি পাচ্ছে। বিশ্বকে জানার অদম্য কৌতুহল নিয়ে কম্পিউটারের সামনে বসছে মেয়েরা। সাইবার স্পেস থেকে প্রাপ্ত তথ্যকে তারা ব্যবাহার করছে তাদের পড়াশুনা ও গবেষণার কাজে। তথ্যসমৃদ্ধ করছে তাদের পরীক্ষার খাতা বা গবেষণাপত্র। কিন্তু সম্প্রতি এ ক্ষেত্রে ব্যাপক বিপত্তিও দেখা দিয়েছে। সাইবার স্পেসে মেয়েদের অংশগ্রহণের সুযোগকে কাজে লাগিয়ে তাদের উত্ত্যক্ত করার প্রবণতা ও বৃদ্ধি পাচ্ছে। এক্ষেত্রে যে জিনিসটি সবচেয়ে বেশি করা হয় তা হলো আপত্তিকর মন্তব্য সম্বলিত মেইল প্রেরণ। বর্তমানে যুক্ত হয়েছে নতুন মাত্রা। বিভিন্ন পর্ণো ছবিতে কোন মেয়ের মুখের লাগিয়ে ছবি তৈরি করে ইন্টারনেটে ছেড়ে দেওয়া হচ্ছে।এসব যারা করে তারা এর বিরুপ প্রতিক্রিয়া সম্পর্কে মোটেও ভাবেনা। বিকৃত এক নেশায় আসক্ত তরুণরাই এ অপরাধের সবচেয়ে বেশি সম্পৃত্ত।আর তাদের এ কাজে উদ্বুদ্ধ করে সাইবার ক্যাফে গুলো নিরিবিলি পরিবেশ। এতে আক্রান্ত হয়ে মেয়েরা যেমন সামাজিকভাবে হেয় প্রতিপন্ন হয়, তেমনি হয়ে পড়ে মানসিকভাবে দূর্বল।

ঙ. সাইবার টেরোরিজম

সাইবার টেরোরিজম। বাংলায় বলা যায়– সাইবার সন্ত্রাস। এই সাইবার সন্ত্রাস বর্তমানে ব্যপক হারে সংঘটিত হচ্ছে। এটা হচ্ছে কম্পিউটার ভিত্তিক অপরাধ যার মাধ্যমে রাজনৈতিক উদ্দেশ্য হাসিলের জন্য জান ও মালের বিনাশ ঘটানো হয়। সাইবার সন্ত্রাসের লক্ষ্য সরাসরি আর্থিক ও মানুষ জনের ক্ষতি সাধন এবং যোগাযোগ ও সার্ভিস ব্যাহত করা। সার্বিক দিক থেকে অবশ্য সত্যিকারের সাইবার সন্ত্রাসের ঘটনা খুবই কম। তবে এই সামান্য সংখ্যক সাইবার সন্ত্রাসী ব্যপক ক্ষয়ক্ষতি ও ধ্বংসযজ্ঞ সাধনের জন্য যথেষ্ট। আজকের আধুনিক দুনিয়ায় সন্ত্রাসের সাথে টেকনোলজি দিন দিন ওতোপ্রোতভাবে জড়িত। সন্ত্রসীদের কার্যকলাপের জন্য তাদের প্রয়োজন হয় দ্রুত কমিউনিকেশনের জন্য এবং তা হতে হয় নির্ভরযোগ্য। আমেরিকা বর্তমানে ওসামা বিন লাদেনের নেটওয়ার্কের তথাকথিত সন্ত্রাসবাদের বিরুদ্ধে যখন সর্বোচ্চ প্রচেষ্টা চালাচ্ছে তাকে খুঁজে বের করার জন্য, সেই সময়ে তারা ইন্টারনেট ও অন্যান্য হাইটেক কমিউনিকেশন ব্যবস্থাকে স্ক্যান করতেও বাকি রাখছে না। ধারনা করা হচ্ছে আমেরিকার এফবিআই বা ফেডারেল ব্যুরো অব ইনভেস্টিগেশন স্যাটেলাইটকেন্দ্রিক এসপিউনাজড নেটওয়ার্ক ব্যবহার করে যা বিশ্বব্যাপি কমিউনিকেশনকে মনিটর করতে পারে। আমেরিকান অথরিটি অবশ্য কখনোই স্বীকার করে না অনুরূপ প্রযুক্তি ব্যবহার বা এই সংক্রান্ত কোন তথ্যকে।

চ. হ্যাক্টিভিজম

হ্যাক্টিভিজম হল কম্পিউটার সিস্টেমে প্রবেশ করে গোপনীয়ভাবে অন্যের তথ্য বা বার্তা অনুমতি ব্যতিরেকেই দেখা কিংবা পরিবর্তন করা।[২৩] সাইবার ক্রাইমের অন্যতম একটি ধরন হল হ্যাক্টিভিজম। বুদ্ধি বৃত্তিক অপরাধীরা এর প্রবর্তন করে। হ্যাক্টিভিস্টরা কৌশলকে কাজে লাগিয়ে অবৈধ কর্মকাণ্ডকে যৌক্তিক করে তোলে। এর শুরু ওয়ার্ল্ড ট্রেড সেন্টারে সন্ত্রাসী হামলার পর। এ ধরনের সাইবার অ্যাটাক রচনা হতে পারে ব্যক্তিগত পর্যায়ে, অথবা এমন কোন গোষ্ঠী পর্যায়ে। দেশপ্রেমের নামে এ অপরাধ কর্মকাণ্ডের সূচনা। সেটা ছিল খুবই দুর্ভাগ্যজনক প্রতিক্রিয়া। যদিও কিছু কিছু হ্যাক্টিভিস্ট বিশ্বাস করে যে তারা সমস্যাকে আরও বাড়িয়ে দিচ্ছে। এদের কর্মকাণ্ড মার্কিন স্বার্থে নেতিবাচক প্রভাব ফেলবে– এমন সম্ভাবনাই বেশি। আগামী সাইবার অ্যাটাকের অধিকাংশই আসবে হ্যাক্টিভিস্টদের কাছ থেকে বলে ধারনা করা হচ্ছে।

ছ. পর্ণোগ্রাফির প্রসার

অশ্লীল চিত্রের ব্যবসায়িক প্রচারণাই হচ্ছে পর্ণোগ্রাফি। অসাধু ব্যবসায়িরা সংকীর্ণ ব্যবসায়িক মনোবৃত্তিতে উলঙ্গ অঙ্গভঙ্গী প্রদর্শনের প্রচেষ্টায় তথ্য প্রযুক্তির মাধ্যমে যে অবাধ প্রসার ঘটাচ্ছেন তাহা পর্ণোগ্রাফির ব্যাপক প্রসার হিসেবে বর্তমান বিশ্বে এক ভয়াবহ অবস্থার সৃষ্টি করেছে। মার্কিন যুক্তরাষ্ট্রের প্রভাবশালী পত্রিকা ফর্বস এর এক সমীক্ষায় দেখা গিয়েছে পর্ণোগ্রাফি এখন ৫৬ বিলিয়ন মার্কিন ডলারের বিশ্ব বাণিজ্য।[২৪] আর এ বাণিজ্যের অন্যতম প্রধান মাধ্যম হলো সাইবার স্পেস। বিভিন্ন বারবনিতাকেন্দ্রের কর্মীদের কুরুচি ও বিকৃত রুচি সম্পন্ন ছবি ছাড়াও অনেক ওয়েব সাইট রয়েছে যেগুলোর মাধ্যমে পর্ণোগ্রাফি ছড়ানো হয়।

বর্তমান উন্মুক্ত তথ্যপ্রযুক্তির যুগে তথ্যকে গণ্ডিবদ্ধ করার প্রয়াস বাতুলতা মাত্র। কিন্তু এমন কিছু বিষয় আছে যা সামাজিক ও উন্নত মানসিকতা দ্বারাই সীমাবদ্ধ করা উচিত। মানুষের আধুনিক মন বা উন্নত মানসিকতা বলে অপসংস্কৃতি ও বিকৃত সংস্কৃতি সর্বদাই পরিতাজ্য। যদিও অনেক কম্পিউটার ব্যবহারকারী এই বিশেষ শ্রেণীর ইন্টারনেট সুবিধাবলী ও ওয়েব পেজের প্রতি আগ্রহী তথাপিও এই পর্ণোগ্রফির প্রতি আকর্ষণ শুধু শক্তিশালী ও উন্নত মানসিকতা দ্বারাই মোকাবেলা করা সম্ভব। প্রাপ্ত বয়স্ক একজন মানুষ নিজস্ব বিচার-বিবেচনা ও মানসিকতা দ্বারা এটা রোধ করতে পারে যদিও এ বিষয়ে প্রাপ্ত বয়স্ক কাউকে

---

[23] New Oxford Advanced Learner's Dictionary 7th edition 2005 (5th impression 2006) Printed in India, see, hack p.695.

Scanned with CamScanner

বিরত রাখতে বলা পরোক্ষভাবে প্রাইভেসি বিরুদ্ধ পর্যায়ে পড়ে। কিন্তু যে সকল ইন্টারনেট ব্যবহারকারী অপরিণত বয়স্ক বা অপ্রাপ্ত বয়স্ক তাদের জন্য এধরণের অবাধ ওয়েব সাইটগুলো খুবই মারাত্মক প্রভাব ফেলে। এধরনের বিকৃত সংস্কৃতির ছোবলে আমাদের কোমলমতি শিশু-কিশোরদের মন-মানসিকতা ও সার্বিক চেতনায় একধরনের প্রতিকূল প্রভাব ফেলে।

উন্নত বিশ্বের প্রায় সবকটি উল্লেখযোগ্য পর্ণোগ্রফিক ওয়েবসাইটে প্রাপ্ত বয়স্কদের সাইটে বিভিন্ন সর্তকতামূলক নিয়মনীতি ছাড়া রয়েছে পৃথক পৃথক বয়স নির্ধারন আইডেনটিটি নাম্বার, যার সাহায্যে ব্যবহারকারীর সাইটটিতে প্রবেশাধিকার সংরক্ষিত হয়। কিন্তু আমদের উপমহাদেশে ও কিছু উন্নয়নশীল রাষ্ট্রের পর্ণোগ্রাফিক ওয়েব সাইটগুলোতে কিন্তু এধরনের সুযোগসুবিধা নেই। এক সমীক্ষায় দেখা গেছে আমাদের ইন্টারনেট ব্যবহারকারীদের মধ্যে মোট ৩৫% ব্যবহারকারী অপ্রাপ্ত বয়স্ক; যাদের বয়স ১০ বছর থেকে ১৮ এর মধ্যে।[২৫] তাই এধরনে ব্যবহারকারীদের নিয়ে আমরা সত্যিকার অর্থেই একটি মারাত্মক সঙ্কটের মুখোমুখি দাঁড়িয়ে কেননা আমাদের নেই কোন সার্টিফিকেশন প্রক্রিয়া। আর তাই বিভিন্ন পেরেন্টাল লক ও পাসওয়ার্ড সফটওয়ারের প্রয়োজন পড়ছে।

জ. বুদ্ধিবৃত্তিক সম্পদের অবৈধ ব্যবহার

কোন লেখক বা প্রকাশক তার নিজের চিন্তা-চেতনা দ্বারা যে সৃষ্টি প্রকাশ করেন তাই তার বুদ্ধিবৃত্তিক সম্পদ।অবাধ তথ্য প্রবাহের সুযোগ নিয়ে অন্যের সৃষ্ট কর্মকে নিজের নামে চালিয়ে দেওয়ার অসাধু প্রবণতা বুদ্ধিবৃত্তিক সম্পদের অবৈধ ব্যবহার হিসেবে পরিগণিত। ইন্টারনেট থেকে এ সম্পদের অধিকার ক্ষুন্ন হওয়ার সম্ভবনা অত্যধিক: 'Intellectual Property is an extraordinary complex subject. We are almost clueless about how to handle digital...works & digital fair use. In a digital World, the bits are endlessly copyable, infinitely, malleably & they never go out of print millions of people simultaneously read any document & they can also steal it.[26]'

চিত্রশিল্প, ভাস্কর, কমপিউটার সফটওয়্যার ডেভেলপার ইত্যাদি হলো বুদ্ধিবৃত্তিক বা মেধাবৃত্তিক সম্পদ। কিন্তু দস্যুতার জন্য মানুষের এই সম্পদের স্বত্ব আজ আর রক্ষা করা যাচ্ছে না। বুদ্ধিবৃত্তিক এসব সম্পদ ডিজিটালি সংরক্ষণ করার ফলে খুব সহজেই এসব সম্পদ এক জায়গা থেকে অন্য জায়গায় প্রেরণ করা হচ্ছে, চুরি-হ্যাক করা হচ্ছে, প্রচার

---

২৪ আনু মুহাম্মদ, 'পুঁজিবাদী বিশ্বায়নের ধারাবাহিকতা ও বৈপরীত্য', সংস্কৃতি, ডিসেম্বর, ১৯৯৯, পৃ. ৩৪।

২৫ প্রাগুক্ত, পৃ. ৩৫।

২৬ Nicholas Negropouts, *A Bill of Rights*, www.bileta.ac.uk

করা হচ্ছে নিজের নামে। এতে বুদ্ধিবৃত্তিক সম্পদের মালিকটি ক্ষতিগ্রস্ত হচ্ছে ব্যাপকহারে, হারিয়ে ফেলছে নতুন কিছু সৃষ্টির উৎসাহ।

৪. বিভিন্ন সময়ে সংঘটিত সাইবার ক্রাইমের চিত্র

সাইবার ক্রাইমের মাত্রা ও হার নাটকীয়ভাবে বেড়ে চললেও আমরা আজ এর ভয়াবহতা বুঝতে ব্যর্থ হচ্ছি। এখনো যথার্থ সিদ্ধান্ত নিতে পারছি না যে এর জন্য আমাদের কতটুকু মেধা, শ্রম ও অর্থ ব্যয় করতে হবে। নিরাপত্তা বিশেষজ্ঞদের মতে সাইবার ক্রাইমের ফলে বিশ্বে প্রতি বছর ক্ষয় ক্ষতির পরিমান প্রায় ৫৫ মিলিয়ন থেকে ১৩ বিলিয়ন মার্কিন ডলার।[২৭]

মার্কিন যুক্তরাষ্ট্রের সুপরিচিত গবেষণা প্রতিষ্ঠান 'Computer Crime And Security Survey' এর সহায়তায় কম্পিউটার ও সাইবার স্পেসে ক্রাইমের উপর গবেষণা পরিচালনা করে। গবেষণার জন্য তারা বেছে নেয় ৪৯৪ টি বিভিন্ন সরকারী প্রতিষ্ঠান, অর্থনৈতিক প্রতিষ্ঠান, মেডিকেল কলেজ ও বিশ্ববিদ্যালয়কে। ২০০৪ সালে পরিচালিত এ গবেষণায় দেখা যায় যে, মাত্র ১২ মাসে কম্পিউটারের অবৈধ ব্যবহারের হার ছিল ৫৩%; যা ১৯৯৯ সালের থেকে ৩৫%বেশি।[২৮] ২০০৪ সালেরই অপর এক পরিসংখ্যান অনুযায়ী সে বছর মার্কিন যুক্তরাষ্ট্রের শতকরা ১২ ভাগ প্রতিষ্ঠানই কম্পিউটার অপব্যবহারের মুখোমুখী হয়।[২৯] আর এ ধারাটি বিশ্বের প্রায় সব দেশেই প্রযোজ্য।

জাপান ও চীনে গবেষণায় সাইবার ক্রাইমের একই রকম চিত্র দেখতে পওয়া যায়। মার্কিন যুক্তরাষ্ট্রে CSI/FBI এর জরিপে দেখা যায় যে, ২০০৩ সালে ৪২% এবং ২০০৪ সালে ৪৯% কম্পিউটার সাইবার আক্রমণের শিকার হয়। এর ফলে বিভিন্ন প্রতিষ্ঠান তাদের গোপনীয়তা, সততা ও তথ্যের প্রবাহমানতা নিয়ে সমস্যায় পড়ে।[৩০] বিশেষজ্ঞদের মতে, কম্পিউটার সম্পর্কীয় অপরাধগুলোর অধিকাংশ ক্ষেত্রে অনুধাবন করতে পারা যায় না; ফলে সঠিক ব্যবস্থা গ্রহণও কঠিন হয়ে পড়ে। কেননা এ ক্ষেত্রে ক্ষতির শিকার ব্যক্তি বা প্রতিষ্ঠানগুলো তাদের এই ক্ষতির পেছনে দায়ী ব্যক্তি বা প্রতিষ্ঠানকে চিহ্নিত করতে পারে না। আর এ কারণে তারা (ক্ষতির শিকার ব্যক্তি বা প্রতিষ্ঠান) এ নিয়ে (সাইবার অপরাধ) গবেষণাকারীদের সঠিক তথ্য দিয়ে সহায়তা করতে পারে না। এক পরিসংখ্যানে দেখা

২৭ Chawki Mohamed, A Critical Lookat the Regulation of Cybercrime, 2005 www.crime.research.org/articles/ Critical/

২৮ ibid.

২৯ ibid.

৩০ ibid.

যায়- সাইবার অপরাধের ক্ষতির শিকার ব্যক্তি বা প্রতিষ্ঠানগুলোর মধ্যে মাত্র১০%টেলিফোনে এবং মাত্র ১% ই-মেইলে সঠিক তথ্য দানে সক্ষম হয়।[৩১]

৫. সাইবার ক্রাইম রোধে জাতীয় ও আর্ন্তজাতিকভাবে গৃহীত আইনগত পদক্ষেপ

অতি সম্প্রতি বাংলাদেশে তথ্য ও যোগাযোগ-প্রযুক্তি আইন- ২০০৬ গৃহীত হয়েছে। এটি ২০০৬ সালের ৩৯ নম্বর আইন। এ-আইনের অষ্টম অধ্যায়েরর ধারা ৫৪, ৫৬ ও ৫৭-তে সাইবার অপরাধ, হ্যাকিং, অশ্লীল ও মানহানিকর চিত্র প্রকাশ এবং সাইবার অপরাধ নিয়ন্ত্রণ ও দমনের জন্য বিধান রাখা হয়েছে। এছাড়াও আইন কমিশন এ বিষয়ে আরো যুগোপযুগী আইন প্রণয়নের জন্য কাজ করে যাচ্ছে। কম্পিউটারের ইতিহাসের সাথে সাইবার ক্রাইমের ইতিহাস জড়িত। সাইবার ক্রাইমের বহু আন্তর্জাতিক ও অতিরাষ্ট্রিক প্রতিষ্ঠান আন্তঃসীমান্তে সাইবার ক্রাইমের বিদ্যমান প্রকৃতিকে স্বীকার করে নিয়েছে। কেননা এ সমস্যা সমাধানে বহুপাক্ষিক প্রচেষ্টার ক্ষেত্রে বেশ কিছু সীমাবদ্ধতা রয়েছে। আর তাই এর জন্য প্রয়োজন ঐক্যবদ্ধ আন্ত-র্জাতিক প্রচেষ্টা এবং প্রযুক্তি আইনের ক্ষেত্রে বিভিন্ন সমস্যার সমাধান। এক্ষেত্রে অগ্রণী ভূমিকা পালন করছে 'ইউরোপীয় কাউন্সিল' এবং 'ইউরোপীয় ইউনিয়ন'। আর এতে সম্প্রতি যোগ দিয়েছে 'ডি-৮' এবং আন্তর্জাতিক পুলিশ সংস্থা 'ইন্টারপোল'। এছাড়া জাতিসংঘও বেশ গুরুত্বপূর্ণ ভূমিকা পালন করছে। সাইবার স্পেসে কম্পিউটার সম্পর্কিত বিভিন্ন সমস্যা সমাধানে এইসব আন্তর্জাতিক ও আন্ত-রাষ্ট্রিক প্রতিষ্ঠানগুলোর সবচেয়ে বড় অবদান হলো- বিভিন্ন ফৌজদারি ও প্রশাসনিক আইনের সমন্বয় সাধন এবং জনসচেতনতা বৃদ্ধি।

সাইবার ক্রাইমের বিষয়টি আলোচনার জন্য ইউরোপীয় কাউন্সিল বিষয়টি নিয়ে বিশেষজ্ঞ পর্যায়ে বেশ আলোচনা-পর্যালোচনা করে। ইউরোপীয় কাউন্সিল কমিটি ৮৯(৯) নামে একটি খসড়া প্রস্তবনা অনুমোদন করে। ১৯৮৯ সালের ১৩ সেপ্টেম্বর পেশকৃত এ প্রস্ত াবনায় সাইবার ক্রাইমের মতো এই নব্য চ্যালেঞ্জ মোকাবেলায় প্রয়োজনীয় তাৎক্ষণিক ব্যবস্থা গ্রহণের প্রতি গুরুত্বারোপ করা হয়। এই অপরাধমূলক কর্মকাণ্ডকে নিষিদ্ধ করে এর একটি সংক্ষিপ্ত তালিকা সদস্য দেশগুলোর কাছে পেশ করা হয়। এছাড়া আরো বেশ কয়েক ধরণের অপরাধমূলক কর্মকাণ্ডকে বর্ণনা করে ঐক্যবদ্ধ আন্তর্জাতিক প্রচেষ্টার কথা বলা হয়। তবে এ প্রস্তবনায় স্বীকার করে নেওয়া হয় যে, এ বিষয়ে আন্তর্জাতিক সমঝোতায় পৌছানো সত্যিই কঠিন। ১৯৯০ সালে জাতিসংঘ কংগ্রেস সাইবার স্পেসে অপরাধমূলক কর্মকাণ্ড হ্রাস ও অপরাধীদের বিরুদ্ধে প্রয়োজনীয় ব্যবস্থা গ্রহণের ক্ষেত্রে বেশ কিছু আইনী বাধা চিহ্নিত করে কম্পিউটার সম্পর্কিত অপরাধের বিরুদ্ধে চলমান যুদ্ধকে

৩১ *Ibid.*

জোরদার করতে নিজস্ব আইনী ব্যবস্থা আধুনিকীকরণ করার জন্য সদস্যদেশগুলোর প্রতি আহ্বান জানায়। এছাড়া ভবিষ্যতে এইসব অপরাধের বিরুদ্ধে আইনী লড়াই চালানোর সুবিধার্থে নিজস্ব নিরাপত্তা ব্যবস্থা জোরদার এবং আন্তর্জাতিক নীতিমালার উন্নয়নের এই ধারাকে এগিয়ে নিতে সদস্য দেশগুলোকে অনুরোধ করা হয়। এর প্রায় দুই বছর পর ইউরোপীয় কাউন্সিল এবং ২৪টি সদস্য দেশ এক সভায় একটি প্রস্তবনা পেশ করে; যাতে সরকারি ও বেসরকারি প্রতিষ্ঠানগুলোর প্রয়োজনীয় তথ্য নিরাপত্তা কাঠামো শক্তিশালী করার উদ্দেশ্যে একটি নির্দিষ্ট নীতিমালার প্রয়োজনীতার কথা বলা হয়। তথ্য নিরাপত্তা কাঠামোর এই নীতিমালাগুলোকে পরবর্তীতে প্রস্তাবনায় সংযুক্ত করে নেওয়া হয়। এতে মূলত সাইবার স্পেসে আচরণবিধি, আইনী বিষয় এবং প্রযুক্তির বিভিন্ন দিকের কথা বলা হয়। যাতে তথ্যের নিরপত্তার জন্য অল্প পরিসরে হলেও এসব নীতিমালার বাস্তব প্রয়োগের প্রতি গুরুত্বারোপ করা হয়। যাহোক, এই নীতিমালায় তথ্যপ্রযুক্তির অপব্যবহাররোধে প্রয়োজনীয় শাস্তির বিধান করে আইন প্রণয়ন ও অন্যান্য প্রশাসনিক পরিকাঠামো উন্নয়নের জন্য সদস্য দেশগুলোর আহ্বান জানানো হয়।[৩২]

কম্পিউটার সম্পর্কিত অপরাধ হ্রাস ও নিয়ন্ত্রণের লক্ষ্যে ১৯৯৫ সালে জাতিসংঘ নিজস্ব একটি ম্যানুয়েল প্রকাশ করে। এই ম্যানুয়েলে মূলত কম্পিউটার সম্পর্কিত অপরাধের ধারণা, ব্যক্তিগত গোপনীয়তা সুরক্ষায় প্রয়োজনীয় অপরাধ আইন এবং আন্তর্জাতিক সহযোগিতা নিয়ে আলোকপাত করা হয়। একই বছর 'ইন্টারপোল' এই ধরণের অপরাধ (কম্পিউটার ক্রাইম) এর উপর একটি সম্মেলন আয়োজন করে। এই সম্মেলনে কম্পিউটার সম্পর্কিত অপরাধরোধে আইন প্রয়োগকারী সংস্থাগুলোর ব্যাপক ভূমিকার কথা বলা হয়। বিষয়টি নিয়ে ব্যাপক আলাপ আলোচনার লক্ষ্যে ইন্টারপোল আরো বেশ কয়েকটি সম্মেলন আয়োজন করে।[৩৩] একই বছর ইউরোপীয় কাউন্সিল সদস্য দেশগুলোর মন্ত্রীদের কমিটিতে 'R(95)13' নামে একটি প্রস্তাবনা পেশ করে। এ প্রস্তাবনার কিছু অংশে কম্পিউটার সম্পর্কিত অপরাধরোধে ব্যাপক অনুসন্ধান চালানো এবং প্রয়োজনে অপরাধীর সরঞ্জামসমূহ জব্দ করার কথা বলা হয়। সর্বপোরি অপরাধীদের তালিকা তৈরি করে আন্তর্জাতিক পরিমণ্ডলে পারস্পরিক সহযোগিতা বৃদ্ধির কথা বলা হয়।[৩৪]

ইউরোপীয় কাউন্সিল ১৯৯৭ সালের ২৪ এপ্রিল সাইবার স্পেসে অবৈধ ও ক্ষতিকর বিষয়াদির উপর নিষেধাজ্ঞা আরোপ করে একটি নীতিমালা প্রস্তুত করে। যাতে বিভিন্ন

---

[৩২] মুনীর, গোলাম, "ওয়ার্ল্ড ট্রেড সেন্টারে হামলা- সম্ভাব্য সাইবার অ্যাটাক ও আমাদের প্রযুক্তি", মাসিক কম্পিউটার জগৎ (২০০১) বর্ষ ১১, সংখ্যা ০৬, পৃ. ২১।

[৩৩] মুনীর, গোলাম,প্রাগুক্ত, পৃ. ২৩।

Scanned with CamScanner

ক্ষেত্রে কমিশনের উদ্যোগে আন্তর্জাতিক সহযোগিতার প্রতি গুরুত্বারোপ করা হয়। চুক্তি অনুযায়ী, এক বছর পর ইউরোপীয় কমিশন কম্পিউটার অপরাধের উপর একটি প্রতিবেদন কাউন্সিলের সামনে উত্থাপন করে। এর এক বছর পর ইউরোপীয় কাউন্সিলের সাইবার ক্রাইম বিশেষজ্ঞ দল সাইবার স্পেসে বিভিন্ন প্রকার অপরাধ রোধে একটা খসড়া ঘোষণাপত্রের রূপরেখা চূড়ান্তকরণের বিষয়টিকে বেশ আন্তরিকতার সাথেই নেয়। কিন্তু এটা ছিল চার বছরের এক দীর্ঘ প্রক্রিয়া এবং এর আগে কমিটির সামনে আরো ২৭ টি খসড়াপত্র উত্থাপণ করা হয়। ২০০১ সালের ২৫ মে ইউরোপীয় কমিটিতে খসড়াপত্রটি জমা দেওয়ার পর ১৮-২২ জুন অনুষ্ঠিত কমিটির ৫০তম পরিকল্পনা সভায় মূল প্রস্তাবনাটি উত্থাপণ করা হয়। যাহোক, এই ঘোষণাপত্রের দ্বিতীয় অনুচ্ছেদেই আলোচিত মূল বিষয়গুলোকে তুলে ধরা হয়। তবে এই অনুচ্ছেদটি আবার দু'টিভাগে বিভক্ত। যার প্রথম ভাগটি স্বতন্ত্রভাবে অপরাধ আইনের উপর'। আর দ্বিতীয় ভাগটি হলো আইনের প্রয়োগ পদ্ধতি নিয়ে। সাইবার স্পেসে সংঘটিত অপরাধগুলোর বিশদ আলোচনার অংশ হিসেবে রচিত এই ঘোষণাপত্রের প্রথম ভাগে মূলত প্রতিরোধ ব্যবস্থা গড়ে তোলার অনুসন্ধান করা হয়। তবে প্রয়োজনে সাইবার স্পেস ছাড়াও এ সম্পর্কিত অপরাধের সাযুজ্য বিধানের প্রতি জোর দেওয়া হয়। এছাড়া সম্মেলনে অংশগ্রহণকারী সদস্য দেশগুলো নিজস্ব আইনের অধীনে প্রয়োজনীয় আইনী ব্যবস্থা গড়ে তুলবে বলে আশাবাদ ব্যক্ত করা হয়। এদিকে ঘোষণাপত্রের অনুচ্ছেদ-২ এর প্রথমভাগে নিম্নলিখিত কর্মসূচী গ্রহণের কথা বলা হয়–

- কম্পিউটারে রক্ষিত গোপন তথ্যের সুরক্ষা ও সহজ প্রাপ্তির ব্যবস্থা;
- কম্পিউটার সম্পর্কিত অপরাধীদের সনাক্ত করা।
- শিশু পর্ণোগ্রাফি রোধ;
- মেধাস্বত্বাধিকার এবং এ সম্পর্কিত অন্যান্য অধিকার কার্যকর করা;
- এইসব অপরাধ কর্মকাণ্ড পরিচালনায় সহায়তা এবং সংগঠিত করার উপর বাধ্যবাধকতা জারি করে নজরদারি বাড়ানো।

সাইবার ক্রাইম নির্মূলের ক্ষেত্রে সম্মিলিত প্রয়াস চালানোর জন্য উপায় খুঁজে বের করতে জি-৮ গ্রুপের পক্ষ থেকে ২০০০ সালের মে মাসে একটি সম্মেলন আয়োজন করা হয়। এতে জি-৮ ভুক্ত দেশগুলো থেকে প্রায় ৩০০ জন বিচারক, পুলিশ কর্মকর্তা, কূটনৈতিক ও ব্যবসায়ী নেতৃবৃন্দ যোগ দেয়। একই বছর অনুষ্ঠিত পরবর্তী সম্মেলনের আলোচ্যসূচীও এ সম্মেলন থেকেই প্রস্তুত করা হয়। ২০০০ সালের জুলাইয়ে অনুষ্ঠিত এ শীর্ষ সম্মেলনে সদস্য দেশগুলোর মাঝে একটি ঘোষণাপত্র জারি করা হয় যাতে বিশ্ব তথ্য সমাজের জন্য

৩৪ প্রাগুক্ত।

হুমকি স্বরূপ এই সাইবার ক্রাইম তথা উচ্চ প্রযুক্তির সকল অপরাধ রোধে ঐক্যবদ্ধ প্রচেষ্টার প্রতি জোর দেয়া হয়।[৩৫]

বিশ্বের প্রায় সব দেশই সাইবার স্পেসের উপর কোন না কোন ভাবে নিয়ন্ত্রন আনতে চায়। পার্থক্য হলো যে তারা কোন ধরনের নিয়ন্ত্রণ প্রতিষ্ঠা করবে। মত প্রকাশের স্বাধীনতায় প্রবলভাবে বিশ্বাসী জার্মানি, বৃটেন, ফ্রান্স ও মার্কিন যুক্তরাষ্ট্রের মতো দেশগুলোও অনাকাঙ্খিত বিষয়ের উপর নিয়ন্ত্রণ আরোপ করে থাকে। এইসব দেশের মধ্যে সর্ব প্রথম যুক্তরাষ্ট্র নিয়ন্ত্রণ আরোপের চেষ্টা চালায়। যুক্তরাষ্ট্র সাইবার পর্ণের কারণে ১৯৯৫ সালে একটা আইন তৈরি করে। ইন্টারনেটে অশোভন বিষয়বস্তুর উপর নিষেধাজ্ঞা আনার জন্য বিল আকারে বিষয়টি উপস্থাপন করেন জেমস এক্সান। কংগ্রেস এটিকে 'কমিউনিকেশন এ্যাক্ট- ৯৫' হিসেবে পাশ করে। এটি আইনে পরিণত হয় ১৯৯৬ সালের ৮ ফেব্রুয়ারি। তবে এক্ষেত্রে এশিয়ার দেশ সমুহের মধ্যে ভারত ইন্টারনেট প্রযুক্তিতে এগিয়ে আছে। ভারত ইন্টারনেটের উপর নিয়ন্ত্রণ আরোপের জন্য ২ সেপ্টেম্বর ১৯৯৬ সালে সিংগাপুরে মিলিত হয়। ভারত কিছু সিদ্ধান্ত নেয়। তাদের প্রধান বিবেচ্য বিষয় ছিল পর্ণোগ্রাফি, সরকারবিরোধী কার্যকলাপ, পশ্চিমা মতাদর্শের ব্যাপক প্রচার ও প্রভাবে এশীয় মূল্যবোধের অবক্ষয়। তারা সকলে মত দেন যে প্রতিটি দেশ নিজেদের মতো করে সাইবার স্পেসে তাদের নিয়ন্ত্রণ প্রতিষ্ঠা করবে। তাদের জাতীয় নিয়ন্ত্রণ ও সাইবার আইন প্রণয়নে অভিজ্ঞতা ও তথ্য আদানপ্রদানের ব্যাপারে পরস্পরের মধ্যে সম্মত হন।[৩৬]

১৯৯৮ সালের ১৫-১৭ এপ্রিল মিডিয়া রেগুলেশন ফর দ্য নিউ টাইমস শীর্ষক এক কর্মশালায় বলা হয় নতুন প্রযুক্তি নিয়ন্ত্রণের জন্য বাস্তব সম্মত ও নমনীয় বিধিমালা গড়ে তোলার উপর গুরুত্বারোপ করা উচিত। চীন ইন্টারনেটের উপর নিয়ন্ত্রণ আরোপের জন্য ১৯৯৬ সালে নতুন আইন প্রবর্তন করে। নতুন আইন অনুসারে প্রত্যেক কম্পিউটার নেটওয়ার্ককে রেজিস্ট্রেশন করতে হবে। এছাড়াও পর্ণোগ্রাফি ও রাজনৈতিক বিষয়বস্তুসমুহের উপর নিষেধাজ্ঞা আরোপ করা হয়। এশিয়ার ইন্টারনেট রাজধানী বলে পরিচিত সিংগাপুর ১৯৯৬ সালের প্রথম দিকে কিছু নীতিমালা প্রণয়ন করে যা ১৯৯৭ সালে পরিমার্জন করা হয়। ভারত ১৯৯৯ সালে 'তথ্যপ্রযুক্তি বিল- ৯৫' প্রস্তুত করে। সে বিলে কম্পিউটার হ্যাকিং, ইলেক্ট্রনিক সন্ত্রাস, অশোভন তথ্য প্রকাশ ইত্যাদির উপর নিষেধাজ্ঞা আরোপ করে।[৩৭] এভাবে বিভিন্ন দেশে বিভিন্ন সময়ে প্রয়োজনের তাগিদে সাইবার ক্রাইম রোধের জন্য চেষ্টা চালানো হয়।

---

[৩৫] রহমান, মোহাম্মদ মাহাবুবুর, প্রাগুক্ত, পৃ: ৩১।

[৩৬] রহমান, মোহাম্মদ মাহাবুবুর, প্রাগুক্ত, পৃ: ৩৩।

[৩৭] প্রাগুক্ত, পৃ.৩৮।

Scanned with CamScanner

যুক্তরাজ্য সরকার সাইবার সন্ত্রাসের হাত থেকে শিশুদের রক্ষার জন্য তাদের বুথগুলোতে শিশুদের 'ভার্চুয়াল প্যানিক বাটন' সরবরাহ করেন। যুক্তরাজ্যের সরকার একটি নীতি মালায় ঘোষণা করেন শিশুদের অবশ্যই ভার্চুয়াল প্যানিক বাটন ও স্বতঃসিদ্ধ নিরাপত্তা বার্তা ওয়েব সাইটের এক কোনায় সব সময়ই দেখাতে হবে।[৩৮] এই নীতমালার আওতায় শিশুদেরও তাদের গুওত্বপূর্ণ তথ্যগুলো চ্যাটরুমের মাধ্যমে আপরিচিত কাউকে না দেওয়ার জন্য অনুরোধ করা হয়েছে। তাদের কয়েক দিন পরপরই পাসওয়ার্ড বদলাতে বলা হয়েছে। সেই সঙ্গে ইন্টারনেট ব্যবহারের সময় কোনো বিপদে পড়লে তাদের কী করতে হবে তা-ও এখানে বলা হয়েছে। এসব নিয়মনীতি সবাইকে জানানোর জন্য সে দেশের সরকার www.thinkuknow.co.uk ঠিকানার ওয়েবসাইট খুলেছে। যুক্তরাজ্য সরকরের এ পদক্ষেপকে স্বাগত জানিয়েছে ইন্টারনেট বিশেষজ্ঞরা।[৩৯]

৬. সাইবার ল'

সাইবার স্পেসকে নিয়ন্ত্রণের জন্য জাতীয় ও আন্তর্জাতিক পর্যায়ে বেশ কিছু আইনগত পদক্ষেপ গৃহীত হয়েছে। তবে 'কপিরাইট আইন কে উল্লেখযোগ্য হিসাবে ধরা হয়। নিম্নে সেগুলোই আলোচিত হল–

ক. কপিরাইট

কপিরাইট বলতে অনেকেই গ্রন্থস্বত্ব বুঝিয়ে থাকেন। কিন্তু এ ধারণাটি সঠিক নয়। মূলত কপিরাইট হচ্ছে শ্রম ও কুশলতার মাধ্যমে মৌলিক কোন সৃষ্টিকর্মের প্রকাশিত ধারণা বা অভিব্যক্তির ওপর একগুচ্ছ একক স্বত্ব বা অধিকার। আর কপিরাইট আইন আসলে বুদ্ধিবৃত্তিক সম্পদের মালিকানা দাবির আইন। কোন লেখকের নিজস্ব সৃষ্টির মুদ্রণ, প্রকাশ, উৎপাদন, পুনর্মুদ্রণ, রূপান্তর, পুনঃপ্রকাশ এবং ব্যবসায়িক স্বার্থে ব্যবহার করার জন্য লেখকের বা রচয়িতার বা সৃষ্টির ওপর স্রষ্টার অধিকারকে সংরক্ষিত করাই কপিরাইট আইনের মূল উদ্দেশ্য।

খ. কপিরাইট আইনের স্বত্বগুলো নিম্নে তুলে ধরা হলো:

- বুদ্ধিবৃত্তিক সম্পদের পূনরুৎপাদনের অধিকার হলো সম্পদটির স্রষ্টার। অন্যকেউ যে সৃষ্টি কর্মের কোনরূপ রূপান্তরের অধিকার রাখে না।
- সৃষ্টকর্মগুলোর প্রকাশ, প্রচার ও বিতরণের অধিকার কেবল স্বত্বাধিকারীর।
- জনসম্মুখে উপস্থাপনের একমাত্র অধিকার সত্বাধিকারীর।
- কোন রচনার চলচ্চিত্রায়ন বা শব্দ রেকর্ড করার অধিকার কেবল রচয়িতা বা স্রষ্টা বা তার প্রতিনিধির।

---

[৩৮] প্রাগুক্ত, পৃ. ৩৩।

[৩৯] *মাসিক কমপিউটার টুমরো*, বর্ষ: ০৪, সংখ্যা ০৪, ফেব্রুয়ারি ২০০৩, ঢাকা। পৃ. ২১।

অভিযোজনের অধিকারও তার।

গ. কপিরাইট লঙ্ঘন

অন্যের সৃষ্টকর্ম নিজের বলে চালানো প্রচার, প্রকাশ, বিতরণ করাই কপিরাইট লঙ্ঘন। বিদেশে কপিরাইটকে অসম্মান করে উৎপাদিত কর্ম দেশে আমদানি করাও কপিরাইট লঙ্ঘন। কপিরাইট লঙ্ঘন জনিত অপরাধে জড়িত হলে সর্বোচ্চ চার বছর কিন্তু ছয়মাসের কারাদণ্ড এবং সর্বোচ্চ ২ লাখ টাকা কিন্তু কমপক্ষে ৫০ হাজার টাকার অর্থদণ্ডে দণ্ডিত হবেন।

৮. সাইবার ক্রাইম প্রতিরোধের উপায়

বর্তমান বিশ্বে যেহেতু হাজারো সাইবার ক্রাইম সংঘটিত হচ্ছে এবং তা প্রতিরোধেরও কোন সুনির্দিষ্ট আইন নেই, সেহেতু তা মোকাবেলা আমাদেরকেই করতে হবে। এর জন্য আমাদেরকেই উদ্যোগী হয়ে কিছু পদক্ষেপ গ্রহণ করতে হবে। এ ধরনের কিছু পদক্ষেপ নিচে দেওয়া হলো:

১. ইন্টারনেট সার্ভিস প্রোভাইডারদের সার্বিক নিরাপত্তা জোরালো করতে হবে;
২. ইলেক্ট্রনিক ব্যবসায় প্রবেশ ও অন্তঃক্রিয়াসহ ভৌত নিরাপত্তার মুল্যায়ন ও পরীক্ষণ করতে হবে;
৩. সাম্প্রতিক সময়ের নিরাপত্তা উপাদান দিয়ে দ্রুত সব ব্যবস্থাকে হালনাগাদ করে নিতে হবে;
৪. প্রতিদিন ভাইরাস সিগনেচার আপডেট করতে হবে;
৫. পেনিট্রেশন টেস্টিং মোকাবেলার ক্ষমতা যাচাইয়ের উদ্যোগ নিতে হবে;
৬. সকল ইনএক্টিভ একাউন্ট নিষ্ক্রিয় করতে হবে;
৭. সম্ভাব্য নিরাপত্তা ভঙ্গের জন্য সাধারণের প্রবেশযোগ্য ওয়েবসাইট অব্যাহতভাবে মনিটর করতে হবে;
৮. ডায়াল-আপ লাইনসমূহ, এক্সট্রারনট ও ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (ভিপিএন) সহ রিমোর্ট এক্সেসের নিরাপত্তা পরীক্ষা করে দেখতে হবে;
৯. সর্বশেষ ও হালনাগাদ প্রবণতার জন্য সিকিউরিটি ডিস্ট্রিবিউশনের লিস্ট করতে হবে;
১০. প্রয়োজনে সিকিউরিটি সার্ভিস প্রোভাইডারের (এমএসএসপি) সাথে যোগাযোগ করতে হবে;
১১. সাইবার কর্মকাণ্ড যাতে না বাড়ে, সে জন্য ব্যবহারকরীদের শিক্ষিত ও সচেতন করে তুলতে হবে;
১২. এক্সটার্নাল সার্ভিস প্রভাইডারদের নিরাপত্তা পর্যালোচনা করতে হবে।[৪০]

গবেষণায় দেখা গেছে, সাধারণ কিছু নিয়ম মেনে চললে ভাইরাস দ্বারা আক্রান্ত হবার সম্ভাবনা ৯৫% কমে যায়। কাজেই আমাদেরকে এ ব্যাপারেও সতর্ক হয়ে কিছু নিয়ম মেনে চলতে হবে। সেসব নিয়মের মধ্যে উল্লেখযোগ্য কিছু নিয়ম নিচে দেওয়া হলো :

---

৪০ গোলাম মুনীর, ওয়াল্ড ট্রেড সেন্টারে হামলা: সম্ভাব্য সাইবার এ্যাটাক ও আমাদের প্রযুক্তি, মাসিক কমপিউটার জগৎ বর্ষ: ১১, সংখ্যা ০৬, অক্টোবর ২০০১, পৃ. ২৯

Scanned with CamScanner

১. যে কোন ডিস্কেট বা সিডি ভাইরাসমুক্ত কি না– এটা না জেনে কখনোই সিস্টেমে কাজ করা উচিত নয়।
২. নিজস্ব ফ্লপি ডিস্ক রাইট-প্রোটেক্ট ট্যাব সেট করে অন্য সিস্টেমে ব্যবহার করতে হবে।
৩. কোন প্রোগ্রাম ইনস্টল করার পূর্বে সেটি ভাইরাসমুক্ত কি না– তা পরীক্ষা করতে হবে।
৪. অখ্যাত বা অপরিচিত বুলেটিন, কোর্ড, নিউজ গ্রুপ ওয়েব সাইট বা নেটওয়ার্ক থেকে সফটওয়্যার বা তথ্য ডাউনলোড করা উচিত নয়।
৫. নিয়ন্ত্রন ছাড়া অন্য কাউকে কমপিউটার ব্যবহার করতে দেওয়া উচিত নয়।
৬. অজানা ই-মেইল অ্যাটাচমেন্ট কখনোই ওপেন করা উচিত নয়।
৭. এন্টি-ভাইরাস এবং অন্যান্য সফটওয়্যারও সর্বদা আপডেট রাখতে হবে।
৮. অনলাইন স্ক্যানিং ব্যবহার করতে হবে।
৯. উন্নতমানের ফায়ারওয়াল ব্যবহার করতে হবে।
১০. পাসওর্য়াড প্রদানের সময় বিচ্ছিন্ন কিছু অক্ষর বা মাঝে মাঝে কিছু সিম্বল (@, #, *) ব্যবহার করতে হবে।
১১. মূল্যবান ডাটাগুলো নিয়মিত ব্যাকআপ করতে হবে।
১২. অলটাইম সফটওয়্যার প্রটোশন ব্যবহার করতে হবে।[৪১]
১৩. অনলাইন অপরাধ সম্পর্কে জনগণের মধ্যে সচেতনতা বৃদ্ধি করতে হবে।
১৪. আর্ন্তজাতিক পর্যায়ে আইন প্রণয়ন ও বাস্তবায়ন করতে হবে।
১৫. আর্ন্তজাতিক চুক্তি সম্পাদন করা যেতে পারে।
১৬. বৈশ্বিক সনদ তৈরি করে তা অনুসরণ করা যেতে পারে।
১৭. অপরাধীদের বিচারের জন্য সাইবার স্পেস কেন্দ্রিক আর্ন্তজাতিক আদালত গঠনের ব্যবস্থা করা যেতে পারে।

শেষ কথা

নতুন নতুন প্রযুক্তির আগমনে বিশ্ব আজ একটা গ্রামে পরিণত হয়েছে। কিন্তু এসব প্রযুক্তির অপব্যবহারে অপরাধও আজ বিশ্বের আনাচে-কানাচে ছড়িয়ে পড়েছে –যার নির্দিষ্ট কোন সীমা রেখা নেই। এসব অপরাধকে নিয়ন্ত্রণের জন্য জাতীয় ও আন্তর্জাতিক পর্যায়ে গৃহীত বিভিন্ন পদক্ষেপের মাধ্যমে আমরা আইনগত প্রতিকার পেতে ও সচেতন হতে পারি। আমরা নিজেদের উদ্যোগেও বিভিন্ন পদক্ষেপ গ্রহণ করে এ ধরণের মারাত্মক অপরাধ থেকে বিশ্বকে রক্ষা করতে পারি। তৈরি করতে পারি অপরাধ মুক্ত সুন্দর পৃথিবী।

---

৪১ প্রাগুক্ত, শোয়েব হাসান খান, ২০০০।

Scanned with CamScanner